Kennis delen geeft kracht

Naar een betere èn zorgvuldigere gegevensuitwisseling in samenwerkingsverbanden

Rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling

Den Haag, 5 december 2014

Inhoudsopgave

Samenvatting

1. Aanleiding

Het kabinet heeft in een brief van 20 december 2013 aan de Tweede Kamer over de aanpak van fraude een verkenning aangekondigd naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding. De vraag die moet worden beantwoord, is of zo'n kaderwet generieke knelpunten met betrekking tot de gegevensuitwisseling in bestaande wetgeving kan oplossen in plaats van het aanbrengen van afzonderlijke wijzigingen in specifieke wetten.

2. Analyse van de problematiek

De behoefte aan een verkenning naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding vloeit voort uit de opvatting van het kabinet dat fraudebestrijding een brede en integrale benadering vergt, waarbij de rijksoverheid samenwerkt met gemeenten en private partijen. Om tot een efficiënte en doeltreffende samenwerking te komen is uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijke en op elkaar afgestemde interventies komen. Partijen ervaren echter knelpunten bij de door hen gewenste gegevensuitwisseling.

Een belangrijke oorzaak van deze knelpunten is gelegen in het feit dat de huidige wetgeving met betrekking tot verwerking van gegevens door overheidsinstanties wordt gedomineerd door regelingen met een sectoraal karakter. Denk hierbij aan de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de bepalingen over gegevensverwerking in bijvoorbeeld de Algemene wet inzake rijksbelastingen. Deze sectorale regelingen houden doorgaans onvoldoende rekening met het bestaan van samenwerkingsverbanden. Dat levert, zoals hierna zal blijken, knelpunten voor de gegevensuitwisseling in die verbanden op.

Deze knelpunten bestaan voor een deel uit wettelijke belemmeringen. Zo vloeien knelpunten bij voorbeeld voort uit het feit dat de bestaande regelingen door hun sectorale karakter onvoldoende duidelijk maken wat bij de gegevensverwerking in een samenwerkingsverband wel en niet mag. Ook voorzien die bestaande bepalingen niet altijd in gewenste vormen van gegevensuitwisseling waardoor sprake is van knelpunten. Deze onduidelijkheden en het ontbreken van wettelijke bepalingen die een grondslag bieden voor gegevensuitwisseling zetten een onnodige rem op de uitwisseling en verdere verwerking van gegevens. Dat belemmert op haar beurt een adequate aanpak van de problemen waarvoor een samenwerkingsverband staat. Voor deze wettelijke belemmeringen kan de vraag worden gesteld of die belemmeringen kunnen worden weggenomen met een kaderwet. Voor een ander deel hangen de bedoelde wettelijke belemmeringen samen met het spanningsveld dat nu eenmaal ontstaat bij een breder gebruik van gegevensuitwisseling en de wettelijke bepalingen die uit een oogpunt van bescherming van privacybelangen van betrokkenen waarborgen bevatten tegen te ver gaande vormen van gegevensverwerking. Deze laatste soort "belemmeringen" zijn van een andere orde dan de eerder genoemde belemmeringen. Bezien wordt in deze verkenning in hoeverre een kaderwet belemmeringen van met name de eerst bedoelde categorie kan wegnemen.

Bij het streven naar verbetering van de mogelijkheden van gegevensuitwisseling zullen kabinet en kamer nadrukkelijk aandacht moeten schenken aan de vraag waar de grenzen liggen bij gegevensuitwisseling. Er dient een afweging te worden gemaakt tussen de belangen die worden gediend met een breder gebruik van gegevensuitwisseling en de in (internationale) regelgeving vastgelegde kaders ter bescherming van de privacybelangen van de burger. In de politieke discussie over de verbetering van de mogelijkheden van gegevensuitwisseling door een kaderwet zullen de relevante belangen scherp in kaart moeten worden gebracht ten behoeve van een verantwoorde belangenafweging en besluitvorming. De Verkenning bevat ten behoeve van deze belangenafweging al de eerste bouwstenen.

3. Aard van de verkenning

De verkenning spitst zich toe op gegevensuitwisseling in samenwerkingsverbanden. Gebleken is dat zich vooral in dergelijke verbanden knelpunten voordoen. Het gekozen uitgangspunt stoelt ook op de gedachte dat gestructureerde vormen van gegevensuitwisseling die niet al in een wettelijke regeling zijn uitgewerkt, meestal binnen een daartoe opgericht samenwerkingsverband plaatsvinden, waarbij de regeling van de gegevensuitwisseling is neergelegd in een convenant en eventueel een protocol.

De verkenning heeft betrekking op gegevensuitwisseling op een breder terrein dan fraudebestrijding. Dat heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uitsluitend fraudebestrijding bezighouden. De tweede reden is dat een eventuele kaderwet evenzeer van belang kan zijn met het oog op knelpunten bij gegevensuitwisseling ten behoeve van andere doeleinden. Gekozen zou dan kunnen worden voor een kaderwet op het brede terrein van de voorkoming van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen, de uitoefening van toezicht op de naleving van wettelijke voorschriften en de handhaving van de openbare orde en veiligheid ("bestuursrechtelijke preventie en handhaving"), alsmede de voorkoming, opsporing en vervolging van strafbare feiten ("strafrechtelijke preventie en handhaving"). Het is immers dit brede terrein waarop zich allerlei samenwerkingsverbanden manifesteren die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen.

Bij een verkenning naar een kaderwet gegevensuitwisseling kan het niet alleen gaan om het verkennen van mogelijkheden om knelpunten weg te nemen die op dit moment met betrekking tot het uitwisselen van gegevens bestaan. Integendeel, een verbetering van de mogelijkheden tot gegevensuitwisseling die uit het wegnemen van deze knelpunten voortvloeit, schept een navenant grote verantwoordelijkheid voor een zorgvuldige inrichting van het proces van gegevensuitwisseling. Het begrip "zorgvuldigheid", uitgewerkt in een aantal waarborgen, zou het centrale ijkpunt bij iedere vorm en fase van gegevensverwerking in samenwerkingsverbanden moeten zijn.

Verbetering van de gegevensuitwisseling in samenwerkingsverbanden is een ambitie die niet alleen met een eventuele kaderwet kan worden gerealiseerd. Daarvoor is ook nodig dat partijen bereid zijn tot samenwerking en het delen van gegevens, daartoe de nodige organisatorische voorzieningen treffen en een adequate (technische) infrastructuur bouwen.

4. Karakter van een kaderwet

Een kaderwet (of raamwet) is een wet die de algemene principes, verantwoordelijkheden en procedures regelt, maar geen gedetailleerde regels bevat. Een belangrijke eigenschap van kaderwetten lijkt dan ook dat zij doorgaans niet zelf beleidsinhoudelijke regulatieve keuzes vastleggen, maar vooral randvoorwaarden scheppen waarbinnen bijvoorbeeld lagere regelgevers, beleidsmakers of uitvoerders dienen te opereren. Een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden zal in dat licht bezien niet voor ieder samenwerkingsverband in detail behoeven te regelen waaraan dat verband zich heeft te houden. Wel zal een kaderwet een raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking nader uitwerken in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. Een kaderwet kan daarbij de knelpunten wegnemen die nu in de praktijk bij het opstellen van zo'n convenant en protocol worden ervaren.

Het uitgangspunt voor een eventuele kaderwet zou zijn dat zij de bestaande regelgeving met betrekking tot gegevensverwerking op enkele uitzonderingen na in stand zou laten. Dat geldt met name ook voor de daarin vastgelegde waarborgen voor de bescherming van persoonsgegevens, zoals het principe van doelbinding en de rechten van burgers van wie gegevens wordt verwerkt

(recht op inzage, correctie en verzet). Een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden zou naast een aantal noodzakelijke afwijkingen of wijzigingen van bestaande wetgeving vooral bestaan uit bepalingen die duidelijkheid moet brengen over wat bij gegevensuitwisseling wel en niet mag, waar de bestaande sectorale wetgeving op de desbetreffende punten onvoldoende helderheid bieden.

Een kaderwet voor gegevensuitwisseling zou een algemene aanvulling vormen op wettelijke regelingen die in specifieke gevallen samenwerking voorschrijven en daarbij regels over gegevensuitwisseling geven, zoals de samenwerking die artikel 9 van de Wet structuur uitvoeringsorganisatie werk en inkomen voorschrijft voor het UWV, de SVB en de gemeenten bij de uitvoering van die wet en enige andere wetten. De aanvullende betekenis van een kaderwet zal zijn gelegen in het feit dat, àls partijen tot samenwerking besluiten en de uitwisseling van gegevens onder de werking van de kaderwet willen laten vallen, deze kaderwet de uitwisseling van gegevens in zo'n samenwerkingsverband legitimeert, faciliteert en normeert. Hiermee is ook gezegd dat de kaderwet niet tot doel heeft een exclusief regime voor gegevensuitwisseling in samenwerkingsverbanden te creëren. Het staat huidige en toekomstige samenwerkingsverbanden vrij ervoor te kiezen hun gegevensverwerking in te richten op grond van de thans al geldende wetgeving.

5. Knelpunten, oplossingen en contouren van een kaderwet

5.1. Van "nee, tenzij" naar "ja, tenzij"

De geheimhoudingsbepalingen in de verschillende bestaande wetten zetten een rem op de gegevensuitwisseling in samenwerkingsverbanden. Door in een kaderwet deze geheimhoudingsbepalingen in relatie tot gegevensuitwisseling in samenwerkingsverbanden buiten toepassing te verklaren, ontstaat ruimte om het huidige uitgangspunt bij de verstrekking van gegevens aan derden, voor samenwerkingsverbanden te transformeren van "nee, tenzij" naar "ja, tenzij".

5.2. Voor gegevensverstrekking aan samenwerkingsverbanden zijn geen afzonderlijke wetswijzigingen meer nodig ...

De ruimte die door het buiten toepassing verklaren van geheimhoudingsbepalingen ontstaat, kan in een kaderwet worden benut door daarin een algemene grondslag op te nemen voor verstrekking van gegevens door de deelnemende partijen aan een samenwerkingsverband. Nu is het voor verstrekking van gegevens aan een samenwerkingsverband vaak nog nodig een specifieke grondslag op te nemen in de desbetreffende wetten en/of daarop gebaseerde uitvoeringsbesluiten. Met zo'n algemene grondslag in de kaderwet is dat niet meer nodig. Op basis van deze algemene grondslag zullen de deelnemers aan een samenwerkingsverband hun samenwerking nader kunnen regelen in een convenant. Daarin zullen zij ingevolge de kaderwet onder meer dienen vast te leggen voor welk doel zij gegevens uitwisselen en hoe zij sturing aan het samenwerkingsverband zullen geven. Uit een oogpunt van "accountability" zou een kaderwet verder moeten voorschrijven dat de deelnemers aan het samenwerkingsverband in een informatieprotocol een aantal in deze wet te noemen elementen vastleggen die bij de gegevensverwerking in een samenwerkingsverband het belang van gegevensbescherming dienen.

5.3. ... maar nog wel een verenigbaarheidstoets

Persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (principe van doelbinding). Dit brengt mee dat voor de gegevensuitwisseling in een samenwerkingsverband moet worden getoetst of zij al dan niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verkregen. De uitvoering van deze toets blijkt in de praktijk bij tijd en wijle een rem te zetten op de bereidheid om gegevens uit te wisselen. Aan het beginsel van doelbinding en daarmee aan de

verenigbaarheidstoets kan echter in het licht van de Europese privacyregelgeving geen afbreuk worden gedaan. Overigens lijkt men in de praktijk soms een te krampachtige houding bij de uitvoering van de verenigbaarheidstoets in te nemen. Dat kan tot het achterwege laten van gegevensuitwisseling leiden, waarvoor een goed uitgevoerde verenigbaarheidstoets wel ruimte zou kunnen geven. Waar op dit punt wetgeving geen uitkomst kan bieden, zou voorlichting dat wel kunnen. Overigens lijkt de nieuwe Algemene verordening gegevensbescherming van de Europese Unie meer ruimte te geven om in de toekomst ook ingeval van onverenigbaarheid van doelen in een samenwerkingsverband toch gegevens te kunnen verwerken.

5.4. Geen twijfel meer over rechtmatigheid van verstrekking aan alle deelnemers tegelijk en aan een eventueel ondersteunend bureau

De huidige wetgeving gaat bij verstrekking van gegevens aan derden doorgaans uit van vormen van bilaterale verstrekking. Er bestaat twijfel of deze wetgeving daarmee ook een voldoende grondslag biedt voor gegevensverstrekking aan alle deelnemers van een samenwerkingsverband tegelijk of aan een eventueel ondersteunend bureau, als dat voor een effectief functioneren van het verband als geheel ten goede zou komen. De kaderwet kan een bepaling bevatten die deze twijfel wegneemt.

5.5. Ruimte voor deelname van private partijen

Publiek-private samenwerking bij fraudebestrijding en de aanpak van andere vormen van wetsovertreding levert beide kanten voordeel op. De bestaande wetgeving geeft echter betrekkelijk weinig ruimte voor gegevensuitwisseling met private partijen. Tenzij een sectorspecifieke wet voor dat geval gegevensverstrekking mogelijk maakt, zal de verstrekking aan een private partij uitsluitend kunnen worden gebaseerd op een bepaling uit de Wet bescherming persoonsgegevens (art. 8, onder f) die een individuele afweging vergt van het gerechtvaardigd belang van de verstrekkende of ontvangende partij tegen het belang van de betrokken burger op bescherming van zijn persoonlijke levenssfeer. Dat belemmert een structurele uitwisseling van gegevens met private partijen. Een eventuele kaderwet zou, onder het stellen van voorwaarden, deze belemmering kunnen wegnemen.

5.6 Verplichte verstrekking van noodzakelijke gegevens, tenzij ...

De deelname aan een samenwerkingsverband kan niet vrijblijvend zijn. De kaderwet zou dan ook moeten voorschrijven dat de deelnemers in beginsel verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens aan de andere deelnemers te verstrekken. Op deze verplichting zou voorshands een uitzondering moeten worden gemaakt, voor zover het om de volgende zgn. bijzondere persoonsgegevens zou gaan: gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakbond. Omdat twee overige categorieën van bijzondere gegevens - strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag – bij uitstek relevant kunnen zijn voor samenwerkingsverband op het brede terrein dat hiervóór onder 3 is beschreven, zouden deze categorieën niet onder voornoemde uitzondering moeten vallen. De verplichting tot gegevensverstrekking zou ook anderszins niet absoluut zijn. Partijen zouden in het informatieprotocol uitzonderingen hierop moeten kunnen opnemen.

5.7. Verstrekking aan opsporingsinstanties en OM wordt eenvoudiger, ...

De samenwerking tussen bestuurlijke en strafrechtelijke instanties kan bij uitstek meerwaarde hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtshandhaving en criminaliteitsbestrijding. Het Wetboek van Strafvordering kent evenwel een systeem voor het vorderen van informatie door opsporingsinstanties en OM, dat een barrière voor een efficiënte vorm van gegevensuitwisseling in samenwerkingsverbanden opwerpt. Het College van procureurs-

generaal heeft in het verleden al op dit probleem gewezen. Door de desbetreffende bepalingen ingeval van gegevensuitwisseling in samenwerkingsverbanden buiten toepassing te verklaren, zal een vordering voortaan niet meer nodig zijn.

5.8 ... verstrekking van strafrechtelijke gegevens ook

In de praktijk bestaat behoefte aan betere mogelijkheden om strafrechtelijke gegevens door politie, bijzondere opsporingsdiensten en OM aan andere partijen binnen het samenwerkingsverband te verstrekken. De bestaande mogelijkheden op dit punt zijn niet optimaal. Zo moest voor verstrekking van politiegegevens aan de Regionale Informatie- en Expertisecentra (RIEC’s) eerst een machtigingsbesluit op grond van de Wet politiegegevens worden afgegeven, volgt later een wijziging van het Besluit politiegegevens en is een en ander ook nog vastgelegd in een convenant en protocol. Op basis van de kaderwet zal volstaan kunnen worden met vastlegging van de verstrekking van politiegegevens, strafvorderlijke gegevens en justitiële gegevens bij convenant en nadere uitwerking daarvan in een informatieprotocol.

5.9 Betere legitimatie van het gebruik van moderne analysetechnieken

Samenwerkingsverbanden worstelen met de vraag of en, zo ja, in hoeverre de huidige regelgeving allerlei typen van gegevensverwerking toestaan. Dat geldt vooral voor het gebruik van geavanceerde analysemethoden. Mag bijvoorbeeld de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV) een door haar te ontwikkelen profiel van bijvoorbeeld beroepsfraudeurs matchen met alle data waarover zij rechtmatig de beschikking heeft, om een lijst vast te stellen van personen aan wie de grootste risico’s zijn verbonden dat zij fraude plegen? De thans bestaande onduidelijkheid op dit punt belemmert de ontwikkeling en het gebruik van diensten en producten die met moderne analysemethoden geleverd kunnen worden. Om de bestaande onduidelijkheid op dit punt weg te nemen, zou een kaderwet kunnen expliciteren dat de door deze kaderwet gereguleerde gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in die wet beschreven typen van gegevensverwerking.

5.10 Vereenvoudiging informatieverstrekking aan burgers

In de praktijk blijkt dat samenwerkingsverbanden zich de vraag stellen of en, zo ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 34 Wet bescherming persoonsgegevens. Die vraag speelt vooral in het geval van geautomatiseerde bestandsvergelijkingen in een fase die voor het overgrote deel van de betrokkenen niet tot gevolgen leidt. Belangrijk is ook dat het in samenwerkingsverbanden op het terrein van de fraudebestrijding al gauw gaat om gegevensverwerking die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden. De informatieplicht geldt niet in het geval dat de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient het samenwerkingsverband de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot vastlegging of verstrekking van de hem betreffende gegevens heeft geleid. Ter compensatie van het wegvallen van de verplichting de burger individueel te informeren, zou een kaderwet kunnen voorschrijven dat bij de oprichting van een samenwerkingsverband ervoor wordt gezorgd dat er algemene informatie wordt gegeven over de gegevensverwerking door het desbetreffende samenwerkingsverband. Deze informatie zou dan bijvoorbeeld op een website van het samenwerkingsverband kunnen worden geplaatst.

5.11. Extra waarborgen voor een zorgvuldige gegevensverwerking

Wil een kaderwet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverbanden opleveren, dan zal deze kaderwet niet alleen een verbetering van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voorzieningen moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan. Daarbij kan onder meer worden gedacht aan explicitering in de kaderwet van het vereiste van

noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit, waarborgen met betrekking tot het koppelen van gegevensbestanden, de duiding van de kwaliteit van de gegevens en de transparantie van de gegevensverwerking en het uitvoeren van een Privacy Impact Assessment.

Uit een oogpunt van “accountability” is het wenselijk dat de kaderwet de deelnemers aan het samenwerkingsverband voorschrijft in een informatieprotocol een aantal elementen vast te leggen die voor de bescherming van gegevens in een samenwerkingsverband van belang zijn. Daarbij kan worden gedacht aan onder meer de volgende elementen: de inrichting van het proces van gegevensverwerking en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens, alsmede de informatieverstrekking over de gegevensuitwisseling aan het publiek en aan betrokkenen.

6. Slot

De werkgroep die deze verkenning heeft opgesteld, heeft niet de pretentie met deze verkenning alles tot in detail te hebben doordacht. Zij heeft wèl de overtuiging dat de verkenning een voldoende basis geeft om een positieve beslissing over het opstellen van een voorstel voor een kaderwet te kunnen nemen.

1. Inleiding

Op 20 december 2013 heeft het kabinet de Tweede Kamer een brief gezonden over de aanpak van fraude met publieke middelen. In die brief kondigt het kabinet onder meer een verkenning aan naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding. De vraag die voorligt, is of zo'n kaderwet generieke knelpunten met betrekking tot de gegevensuitwisseling in de bestaande wetgeving kan oplossen in plaats van het aanbrengen van afzonderlijke wijzigingen in specifieke wetten.[1]

In § 2 van deze verkenning wordt eerst de context geschetst waarbinnen zij heeft plaatsgevonden. In § 3 wordt een aantal knelpunten in de huidige praktijk van gegevensuitwisseling op een rijtje gezet die tijdens de verkenning naar voren zijn gekomen. Vervolgens worden in § 4 de contouren van een mogelijke kaderwet geschetst waarmee deze knelpunten zouden kunnen worden opgelost. De notitie eindigt met een slotbeschouwing (§ 5).

De verkenning is opgesteld door een werkgroep, bestaande uit vertegenwoordigers van de ministeries van Veiligheid en Justitie, Sociale Zaken en Werkgelegenheid en Financiën, van het openbaar ministerie en van de gemeente Tilburg. De werkgroep heeft daarbij in de eerste plaats gebruik gemaakt van ervaringen die zijn opgedaan bij de ontwikkeling van samenwerkingsverbanden waarin partijen gegevens uitwisselen. Verder heeft de werkgroep in april 2014 een brainstormsessie met verschillende genodigden gehouden over knelpunten in de gegevensuitwisseling en de mogelijkheden die een kaderwet zou kunnen bieden om deze op te lossen. Ook heeft de werkgroep voor haar verkenning gebruik gemaakt van de in eerdergenoemde kabinetsbrief aangekondigde inventarisatie van de behoefte aan gegevensuitwisseling in een viertal casussen: gefingeerde dienstverbanden, faillissementsfraude, identiteitsfraude en notoire fraudeurs/subjectgerichte fraudebestrijding. Bij deze inventarisatie is ook naar eventuele knelpunten bij de gegevensuitwisseling gekeken. Voor de verkenning heeft uiteraard ook raadpleging plaatsgevonden van relevante literatuur, officiële publicaties en websites. Concepten van de verkenning zijn gepresenteerd aan verschillende gremia[2] om te toetsen of een eventuele kaderwet uitkomst zou kunnen bieden. De reacties in die gremia waren in het algemeen positief.

In deze verkenning wordt ervan uitgegaan dat de gegevensuitwisseling in enigerlei vorm van samenwerkingsverband plaatsvindt. Daarmee wordt gedoeld op de situatie dat twee of meer partijen voor een bepaald doel in een georganiseerd verband samenwerken en om dat doel te bereiken gegevens uitwisselen. Het is vooral in dergelijke samenwerkingsverbanden dat zich knelpunten laten gevoelen als in § 3 zijn beschreven. Het gekozen uitgangspunt stoelt ook op de gedachte dat gestructureerde vormen van gegevensuitwisseling die niet al in een wettelijke regeling zijn uitgewerkt, meestal binnen een daartoe opgericht samenwerkingsverband plaatsvinden, waarbij de regeling van de gegevensuitwisseling is neergelegd in een convenant en eventueel een protocol. De gerichtheid op samenwerkingsverbanden sluit overigens niet uit dat een eventuele kaderwet ook betekenis kan hebben voor gegevensuitwisseling in "reguliere processen". Gegevensuitwisseling in dergelijke processen kan immers zeer wel vorm krijgen in samenwerkingsverbanden. De gerichtheid op samenwerkingsverbanden brengt wel mee dat verstrekking van gegevens met een incidenteel karakter buiten de reikwijdte van deze notitie vallen. Daar komt bij dat een kaderwet zich minder goed leent voor de oplossing van een eventueel knelpunt bij dat type verstrekking. Zo'n kaderwet zal namelijk al gauw een aantal randvoorwaarden voor gegevensuitwisseling bevatten die niet bij incidentele verstrekkingen passen, zoals de verplichting om een convenant en een informatieprotocol op te stellen (zie nader § 4).

---

[1] Kamerstukken II 2013-2014, 17050, nr. 450, blz. 7-8.

[2] Presentaties zijn gegeven aan o.a. het Landelijk Platform Geïntegreerde aanpak Ondermijnende Criminaliteit en aan het RIEC-hoofden-overleg.

Een kaderwet zou het voordeel hebben dat zij voor allerlei vormen van gegevensuitwisseling één aanvullend kader zou bieden. Het zou dan niet nodig zijn om voor een specifieke vorm van gegevensuitwisseling door middel van een afzonderlijke wet of een afzonderlijk besluit de noodzakelijke wijzigingen in de diverse relevante regelingen aan te brengen. Als een kaderwet, zoals hierna wordt bepleit, betrekking zou hebben op gegevensuitwisseling in samenwerkingsverbanden, zou bovendien de situatie ontstaan dat een samenwerkingsverband als bedoeld in de kaderwet een aangrijpingspunt zou kunnen vormen voor bepalingen in de sectorale wetten die de verstrekking van gegevens aan het samenwerkingsverband regelen. Overigens zou het niet per se noodzakelijk zijn dergelijke bepalingen in de sectorale wetten op te nemen: de kaderwet zelf zou ook kunnen volstaan als basis voor de verstrekking van gegevens aan samenwerkingsverbanden.

Tot slot is van belang dat de verkenning betrekking heeft op gegevensuitwisseling op een breder terrein dan fraudebestrijding. Dat heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uitsluitend fraudebestrijding bezighouden (zie § 2.3). De tweede reden is dat een eventuele kaderwet evenzeer van belang kan zijn met het oog op knelpunten bij gegevensuitwisseling ten behoeve van andere doeleinden (zie nader § 4.2).

2. Context verkenning

2.1 Aanleiding verkenning

Fraude met overheidsvoorzieningen is een groeiend probleem. De effecten daarvan reiken verder dan alleen de directe financiële schade voor de overheid. Fraude ondermijnt de integriteit van het economisch stelsel, het vertrouwen in de financiële instellingen, tast de betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgevoel. Tegen die achtergrond wil het kabinet fraude zoveel mogelijk voorkomen en waar fraude ondanks alle maatregelen toch nog heeft plaatsgevonden, zo effectief mogelijk bestrijden. Dat vraagt volgens het kabinet om een brede en integrale benadering waarbij de rijksoverheid ook zal samenwerken met gemeenten en private partijen, zoals banken en curatoren.[3]

In de praktijk wordt in het kader van fraudeaanpak al veelvuldig samengewerkt door verschillende partijen. Om tot een efficiënte en doeltreffende samenwerking te komen is uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijke en op elkaar afgestemde interventies komen. Daarbij valt in de praktijk een toenemende inzet op "intelligence" en een risico-gestuurde benadering waar te nemen. Dat draagt bij aan de identificatie van personen en organisaties die achter de schermen de regie over zware vormen van fraude voeren, en aan een effectieve inzet van de beschikbare capaciteit om fraude te voorkomen en bestrijden.

Bij de uitwisseling van informatie worden ook persoonsgegevens gedeeld. Het delen daarvan moet uiteraard voldoen aan de wettelijke bepalingen ter bescherming van persoonsgegevens. Hetzelfde geldt voor andere gegevens die wettelijk bescherming genieten. Waar onze wetgeving in algemene zin belangrijke waarborgen voor de bescherming van dergelijke gegevens bevatten, blijken zij echter in de specifieke situatie waarin partijen in samenwerkingsverbanden gegevens willen uitwisselen, de nodige knelpunten op te leveren.

Deze knelpunten belemmeren het optreden van een overheid als een georganiseerd geheel, dat maatschappelijke vraagstukken als de aanpak van fraude integraal, effectief en efficiënt weet op te pakken. De samenleving verwacht echter van een overheid dat zij wel als zo'n georganiseerd geheel optreedt. Zo'n overheid neemt het oplossen van een maatschappelijk probleem als uitgangspunt, kijkt welke overheidsorganisaties en eventueel private partijen nodig zijn om dat probleem te kunnen aanpakken, beziet welke informatie-uitwisseling daarvoor noodzakelijk is en maakt goede afspraken over privacybescherming. De verwachting in de samenleving dat een overheid als een georganiseerd geheel optreedt, neemt ook toe. De ontwikkelingen op het terrein van ICT bieden partijen binnen de overheid immers steeds meer mogelijkheden om tot een snelle, accurate en volledige uitwisseling van informatie te komen en op grond van deze informatie analyses te maken die tot een integraal en effectief optreden leiden. Een verkenning van de mogelijkheden om met een kaderwet tot een betere gegevensuitwisseling te komen, moet dan ook een overheid die langs deze lijnen opereert, als uitgangspunt nemen.

2.2 Dilemma's bij streven naar betere gegevensuitwisseling

Hiervoor is aangegeven dat deze verkenning erop is gericht knelpunten bij de gegevensuitwisseling ten behoeve van de fraudebestrijding in kaart te brengen en te bezien in hoeverre een kaderwet die kan wegnemen. Gebleken is dat de problematiek bij gegevensuitwisseling niet beperkt is tot het domein van fraudebestrijding. In feite blijken de geconstateerde knelpunten zich even goed voor te doen op andere terreinen waar behoefte bestaat aan een ruimer gebruik van gegevensuitwisseling. Dit is derhalve een eerste dilemma: welk bereik dient een Kaderwet gegevensuitwisseling te hebben?

---

[3] Kamerstukken II 2013-2014, 17050, nr. 450, blz. 2.

Bij de behoefte aan een breder gebruik van gegevens speelt voorts als dilemma dat de bestaande regelgeving op het gebied van bescherming van privacybelangen van burgers daaraan grenzen stelt. Waar die grenzen precies liggen is overigens vatbaar voor interpretatie. In de mate waarin een ruimer gebruik van gegevensuitwisseling wordt gemaakt, is duidelijk dat in beginsel eerder tegen grenzen wordt aangelopen en dat meer gefundeerde afwegingen dienen te worden gemaakt. Dat deze belangenafweging noodzakelijk is, is recent nog gebleken bij de vragen die vanuit de Eerste Kamer en Tweede Kamer zijn gesteld over het verzamelen van gegevens door de Belastingdienst en het uitwisselen van die gegevens met andere overheidsorganisaties[4] en over het gebruik van SyRI[5].

Als voorbeeld van de hier bedoelde dilemma's en belangenafweging kan worden gewezen op de geheimhoudingsplicht van bij voorbeeld de Belastingdienst. Deze geheimhoudingsplicht strekt vanouds ertoe dat de belastingplichtige niet wordt belemmerd zijn voor de goede belastingheffing relevante gegevens aan de Belastingdienst te verstrekken in de wetenschap dat de Belastingdienst deze gegevens in beginsel niet aan derden verstrekt. Naast het belang van het heffen van de juiste belasting is hiermee het privacybelang van de burger gediend. Wat betreft het aanleveren van gegevens door ondernemingen is dit privacybelang hierin gelegen dat hun fiscale gegevens veelal bedrijfsgeheimen omvatten, zoals productieprocessen, winstmarges, omzetten en dergelijke. Met zorgvuldige verwerking van dergelijke gegevens door de Belastingdienst is uiteindelijk het belang van Nederland als gunstig vestigingsland voor het internationale bedrijfsleven gemoeid. Dit voorbeeld geeft aan dat naast de belangen die kunnen zijn gemoeid met een breder gebruik van gegevens andere eveneens gerechtvaardigde belangen zich daartegen kunnen verzetten.

Andere dilemma's die bij deze discussie spelen, zijn bij voorbeeld de rol van het vorderingsrecht van het OM en de bijzondere vraagstelling die zich voordoet bij de overgang van gegevens uit het bestuursrechtelijke circuit naar het strafrechtelijke circuit. Beide sferen kennen veelal hun eigen aparte regelgeving. Het strafrechtelijke circuit kent veelal aparte waarborgen in verband met het feit dat in het algemeen bij bemoeienis van het OM sprake is van een verdachte en een vermoeden van een strafbaar feit. Verdragen stellen dan voorwaarden aan het optreden van het OM. Samenwerkingsverbanden die gericht zijn op fraudebestrijding, opereren op het snijvlak tussen het bestuursrecht en het strafrecht. Dit levert nieuwe vragen op, bij voorbeeld de vraag of de gegevensverwerking in zo'n samenwerkingsverband zich onder het regime van de Wet bescherming persoonsgegevens afspeelt dan wel het regime van Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.

In dit verband doet zich voorts de problematiek voor dat met intensivering van samenwerkingsvormen waaraan het OM deelneemt, het OM zich actiever dan voorheen bezig gaat houden met dat deel van zijn taak dat is gelegen op het gebied van het voorkomen van overtredingen. Immers ten tijde van de gegevensuitwisseling in het kader van het samenwerkingsverband is veelal nog niet sprake van de klassieke verdachte en een concreet vermoeden van een strafbaar feit. Dat een dergelijke ontwikkeling de behoefte aan een bezinning op een dergelijke verschuiving van taken van het OM met zich brengt, kan ook als een dilemma worden aangemerkt.

Een en ander impliceert dat in een discussie over eventuele uitbreiding van de mogelijkheden van gegevensuitwisseling door een kaderwet alle relevante belangen en zich voordoende dilemma's scherp in beeld dienen te worden gebracht en goed moeten worden afgewogen. Zonder een gedegen afweging kan van een evenwichtige basis onder een eventuele kaderwet geen sprake zijn. Het streven moet er daarbij op zijn gericht dat in zo'n kaderwet een optimale balans tussen de verschillende belangen wordt gezocht. Het is ook om die reden dat een kaderwet de nodige

---

[4] Zie kamerstukken II 2014-2015, 32761, nr. 71.
[5] Zie Aanhangsel kamerstukken II 2014-2015, 428 en 429.

waarborgen voor een zorgvuldige gegevensverwerking dient te bevatten. Dat kan eraan bijdragen dat ook bij de inrichting van een samenwerkingsverband zelf de optimale balans tussen de verschillende relevante belangen wordt verkregen.

2.3 Samenwerkingsverbanden

Om de effectiviteit van het overheidshandelen te vergroten, richten overheidsorganisaties in toenemende mate samenwerkingsverbanden op. We zien dat niet alleen gebeuren bij de aanpak van fraude, maar ook op andere beleidsterreinen. Wat daarbij opvalt, is dat enkele samenwerkingsverbanden zich in het bijzonder met de aanpak van fraude bezighouden en andere samenwerkingsverbanden een bredere taak hebben, die evenwel ook in enigerlei vorm mede de aanpak van fraude omvat. Dat moge blijken, als we hierna in vogelvlucht een aantal samenwerkingsverbanden de revue laten passeren.[6]

De Belastingdienst, de Inspectie SZW, het UWV, de gemeenten, het OM, de SVB, de ministeries van Financiën en van Sociale Zaken en Werkgelegenheid en de politie werken samen in een interventiestructuur met het oog op het voorkomen en bestrijden van fraude. Het gaat daarbij om belasting- en premiefraude, uitkeringsfraude, illegale tewerkstelling en de daarmee samenhangende misstanden. Deze partijen hebben daartoe in 2003 een samenwerkingsovereenkomst[7] gesloten (de politie is later toegetreden). De interventiestructuur bestaat uit een landelijke stuurgroep, een analysefunctie, regionale platforms en interventieteams. In deze structuur werken de partners niet alleen op strategisch, tactisch en operationeel niveau samen, maar delen ze ook gegevens met elkaar. Het betreft niet alleen gegevensuitwisselingen die casus-gebonden zijn, maar ook gestructureerde bestandskoppelingen op basis waarvan met de inzet van het instrument Systeem Risico Indicatie (SyRI) risicoanalyses worden uitgevoerd en eventuele interventies worden voorbereid.[8]

Om de integriteit van de financiële sector te versterken is in 1998 het samenwerkingsverband Financieel Expertise Centrum (FEC) opgericht. Aan dit samenwerkingsverband nemen de volgende partijen deel: de AIVD, de AFM, de Belastingdienst, DNB, de FIOD, de politie en het OM. Het FEC heeft tot taak een structurele informatie-uitwisseling tussen de partners te creëren, een kenniscentrum te realiseren en projecten uit te voeren. Het FEC richt zich als bewaker van de financiële integriteit op onder meer de volgende aandachtsgebieden: witwaspraktijken, vastgoedfraude, identiteitsfraude, hypotheekfraude, beleggingsfraude en cybercrime.[9] De manier waarop de FEC-partners samenwerken en met elkaar informatie uitwisselen is vastgelegd in een convenant, respectievelijk informatieprotocol.[10]

In 2013 hebben verschillende partijen de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV) opgericht. Het betreft het OM, de politie, de Belastingdienst, de Douane, de FIOD en de Financial Intelligence Unit Nederland. Doel van iCOV is het in kaart brengen van onverklaarbaar of crimineel vermogen, het blootleggen van witwas- of fraudeconstructies en het kunnen innen van overheidsvorderingen ter ondersteuning van de publiekrechtelijke taakuitoefening van de deelnemende organisaties. Met dat doel voor ogen houdt iCOV zich onder meer bezig met het opstellen van rapportages, criminaliteitsbeeldanalyses, risico-indicatoren en groepsprofielen. Een en ander is vastgelegd in een convenant en protocollen.[11]

---

[6] Voor een uitgebreider overzicht van samenwerkingsverbanden wordt verwezen naar bijlage 1.
[7] Zie: http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/belastingdienst_interventieteams.
[8] Kamerstukken II 2012-2013, 33579,, nr. 3, blz. 3.
[9] Zie: http://www.fec-partners.nl/nl/organisatie.
[10] Zie Convenant FEC 2009, Stcrt 2009, 71, en Informatieprotocol FEC 2011, Stcrt. 2011, 21708.
[11] Zie Convenant iCOV 2013, Stcrt 2013, 24607, Protocol gegevensverwerking iCOV Productie 2013, Stcrt 2013, 24608, en Protocol gegevensverwerking iCOV Research and Development 2013, Stcrt. 2013, 24610.

Met het oog op de versterking van de bestuurlijke aanpak en de ondersteuning van de integrale aanpak van de georganiseerde criminaliteit zijn in de afgelopen jaren de Regionale Informatie- en Expertisecentra (RIEC's) en het Landelijk Informatie- en Expertisecentrum (LIEC) opgericht. Binnen de RIEC's en het LIEC werken de volgende partijen samen: de gemeenten, het OM, de politie, de Belastingdienst, de Douane, de FIOD, de Inspectie SZW, de provincies, de Koninklijke Marechaussee en de IND. De samenwerking heeft tot doel gezamenlijk invulling te geven aan

1. een bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit door naast strafrechtelijke ook bestuursrechtelijke en fiscale maatregelen te treffen,
2. de identificering van gelegenheidsstructuren binnen die economische sectoren en publieke voorzieningen die vatbaar zijn voor beïnvloeding door de georganiseerde criminaliteit,
3. de bestrijding van zgn. handhavingsknelpunten en
4. de bevordering en ondersteuning van integriteitsbeoordelingen door het openbaar bestuur op grond van de Wet Bibob.

De samenwerking richt zich voor de eerste twee doelen op onderwerpen als mensenhandel, georganiseerde hennepteelt en fraude in de vastgoedsector. De samenwerking is vastgelegd in een bestuurlijk akkoord en een convenant.[12] De verwerking van persoonsgegevens binnen de RIEC's zal nader worden geregeld in een privacyprotocol.

Naast samenwerkingsverbanden waaraan uitsluitend overheidspartijen deelnemen, ontstaan in toenemende mate samenwerkingsverbanden waarin ook private partijen participeren. Publiek-private samenwerking levert beide kanten voordelen op. De overheid leert van de private sector. Zo zit er veel kennis bij het bedrijfsleven over nieuwe ontwikkelingen, risico's en technologieën. Omgekeerd steekt de private sector ook veel op van de overheid. De samenwerking levert niet in de laatste plaats voordeel op door gebruik te maken van elkaars informatie. Ook private partijen beschikken over informatie die voor het voorkomen en bestrijden van fraude en andere vormen van criminaliteit van belang is. Zowel de private partij als de publieke partij kan op basis van uitgewisselde informatie actie ondernemen of een interventie plegen die bijdraagt aan het voorkomen en bestrijden van criminaliteit. Om een aantal verbanden te noemen: energiebedrijven bij de aanpak van hennepkwekerijen, curatoren bij het voorkomen van faillissementsfraude, financiële dienstverleners bij het tegengaan van witwassen en transportondernemingen bij de handel in verboden goederen.

Ook publieke en private partijen werken vaak met elkaar samen op basis van convenanten. Enkele voorbeelden van dergelijke convenanten zijn:

1. Convenant verbetering bestrijding zorgfraude tussen de Nederlandse Zorgautoriteit, de Inspectie voor de Gezondheidszorg, Zorgverzekeraars Nederland, de Inspectie SZW, de FIOD, de Belastingdienst, het OM, het Centrum Indicatiestelling Zorg en het Ministerie van VWS[13],
2. Convenant hennepteelt Zeeland - West-Brabant 2013 tussen gemeenten, politie, OM, woningcorporaties, netbeheerders, UWV en SVB[14],
3. Convenant aanpak verzekeringsfraude tussen Verbond van Verzekeraars, zorgverzekeraars, het OM en de politie[15].

---

[12] Zie het Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde
Misdaad van september 2008 (kamerstukken II, 29 911, nr. 27) en het Convenant ten behoeve van bestuurlijke en geïntegreerde aanpak georganiseerde criminaliteit, bestrijding handhavingsknelpunten en bevordering integriteitsbeoordelingen (http://download.belastingdienst.nl/belastingdienst/docs/convenant_liec_riec_al11121z1ed.pdf).

[13] Zie: http://www.rijksoverheid.nl/documenten-en-publicaties/convenanten/2013/03/07/convenant-verbetering-van-bestrijding-zorgfraude.html.

[14] Zie: http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/hennepteelt/13.004679-convenant-hennepteelt-zeelandwest-brabant-2013.pdf. Omdat het exploiteren van hennepkwekerijen vrijwel altijd gepaard gaat met andere strafbare feiten zoals diefstal van elektriciteit, belastingontduiking en uitkeringsfraude, richt de samenwerking zich ook op deze vormen van criminaliteit.

[15] Zie:
https://www.verzekeraars.nl/overhetverbond/zelfregulering/Documents/Convenanten/Convenant_aanpak_verzekeringsfraude.pdf.

Het delen van informatie tussen publieke en private partijen ligt gevoelig. Immers, burgers mogen ervan uitgaan dat informatie die zij aan de overheid verstrekken niet zo maar bij private partijen terecht komt. Andersom geldt dat verstrekking van gegevens door private partijen aan de overheid het gevoel kan oproepen van "big brother is watching you". Een (wettelijke) grondslag voor het uitwisselen van gegevens tussen publieke en private partijen ontbreekt vaak.[16] Indien een kaderwet gegevensuitwisseling mede betrekking zou moeten hebben op gegevensuitwisseling tussen publieke en private partijen, dan ligt het voor de hand dat deze wet de nodige waarborgen tegen onwenselijke doelen van gegevensverwerking bevat. Welke dat zouden kunnen zijn, komt in § 4.2 aan bod.

Van de hier genoemde samenwerkingsverbanden houdt een minderheid zich uitsluitend met fraudebestrijding bezig. De meeste samenwerkingsverbanden hebben een taak die zich in meerdere of mindere mate ook tot andere terreinen uitstrekt. Met dat aspect zal rekening moeten worden gehouden bij de overwegingen rond de reikwijdte van een eventuele kaderwet. Een kaderwet die zich beperkt tot gegevensuitwisseling ten behoeve van de fraudebestrijding zal tot gevolg hebben dat verschillende samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van de kaderwet vallen. Op de vraag welke consequentie daaraan verbonden zou kunnen worden, wordt hierna ingegaan in § 4.2.

Tot slot is van belang te onderkennen dat deelnemers aan samenwerkingsverbanden weliswaar gegevens uitwisselen ten behoeve van bijvoorbeeld het formuleren van een gezamenlijke interventiestrategie of het opstellen van bepaalde informatieproducten waaraan gezamenlijk behoefte bestaat, maar vervolgens op basis daarvan onder eigen verantwoordelijkheid en met gebruikmaking van de eigen bevoegdheden eventueel acties ondernemen. Anders gezegd: een samenwerkingsverband laat de bestaande verantwoordelijkheden en bevoegdheden van de deelnemers op dit punt in stand.

2.4 Verschillende wettelijke kaders en categorieën gegevens

Overheidsinstanties en eventueel private partijen verwerken in samenwerkingsverbanden verschillende categorieën gegevens. De categorie die daarbij doorgaans de meeste aandacht krijgt, betreft *persoonsgegevens*. Die aandacht vloeit voort uit het feit dat het bij persoonsgegevens om gegevens gaat die grondrechtelijke bescherming genieten op basis van internationale verdragen, regelingen van de Europese Unie en onze eigen Grondwet.[17] De bescherming van persoonsgegevens is nader geregeld in de Wet bescherming persoonsgegevens (Wbp) als algemeen kader voor de verwerking van persoonsgegevens en daarnaast in sectorspecifieke regelingen als de Wet politiegegevens (Wpg)[18] en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

[16] Zo mag de Belastingdienst op grond van artikel 43c, eerste lid, van de Uitvoeringsregeling Algemene wet rijksbelastingen alleen gegevens verstrekken aan bestuursorganen. Een uitzondering op het beginsel dat geen gegevens aan private partijen mogen worden verstrekt, is te vinden in de Aanwijzing Wet justitiële en strafvorderlijke gegevens van het College van procureurs-generaal. Zo kunnen ten behoeve van het voorkomen en opsporen van strafbare feiten strafvorderlijke gegevens worden verstrekt aan bepaalde "gevoelige" bedrijven of instellingen op het gebied van bijvoorbeeld vervoer en transport, telecommunicatie en internet, beveiliging, financiën, onderzoek, onderwijs, kinderactiviteiten, energie, voedselvoorziening, kunst en oudheden.

[17] Zie artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM), het Dataprotectieverdrag uit 1981 (Trb. 1988, nr. 7), de Europese Privacyrichtlijn uit 1995 (Richtlijn 95/46/EG, Pb L 281), artikel 8 van het Handvest van de grondrechten van de Europese Unie (Pb EG 18 december 2000, C 364/3) en artikel 10 van de Grondwet.

[18] De Wpg is niet alleen van toepassing op politiegegevens. Op grond van artikel 46 Wpg is deze wet van overeenkomstige toepassing op de verwerking van persoonsgegevens door bijzondere opsporingsdiensten.

In de Wbp wordt een persoonsgegeven aangemerkt als elk gegeven betreffende een geïdentificeerde of identificeerbare persoon. Het gegeven dient dus informatie over een persoon te bevatten. Bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen zal dat uit de aard van de gegevens voortvloeien. Maar ook telefoonnummers, kentekens van auto's en postcodes met huisnummers dienen onder omstandigheden als persoonsgegeven te worden aangemerkt.[19]

De Wbp definieert bepaalde gegevens als *bijzondere persoonsgegevens*. Voor dergelijke persoonsgegevens geldt een apart regime. Het gaat om gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakbond, strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. De verwerking van dergelijke gegevens is verboden, tenzij de wet een uitzondering schept. Zo'n uitzondering bestaat bijvoorbeeld voor strafrechtelijke persoonsgegevens, indien de verantwoordelijke de gegevens heeft verkregen krachtens de Wpg of de Wjsg (artikel 22, eerste lid, Wbp).

Politiegegevens zijn persoonsgegevens die in het kader van de uitoefening van de politietaak worden verwerkt. Strafvorderlijke gegevens zijn gegevens die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het OM in een strafdossier of langs geautomatiseerde weg verwerkt. Bij justitiële gegevens gaat het om bepaalde beslissingen van de rechter of het OM ten aanzien van bepaalde personen. Bij zowel strafvorderlijke als justitiële gegevens gaat het overigens niet alleen om persoonsgegevens, maar ook om gegevens over een rechtspersoon. Van belang is verder dat, wanneer gegevens op grond van de Wpg of de Wjsg aan partners in een samenwerkingsverband zijn verstrekt en vervolgens binnen dat verband worden doorverstrekt, die twee wetten niet meer van toepassing zijn en de Wbp geldt.[20]

Samenwerkingsverbanden verwerken uiteraard niet alleen persoonsgegevens. Een andere categorie gegevens waaraan gedacht kan worden, betreft *bedrijfs- of fabricagegegevens.* Het gaat hier om gegevens die bijvoorbeeld in het kader van de uitoefening van toezicht zijn verzameld.[21] Deze gegevens hebben vaak een vertrouwelijk karakter. Verder valt te wijzen op gegevens die uitsluitend voorwerpen aanduiden, bijvoorbeeld gestolen goederen of identiteitsbewijzen. Dergelijke gegevens zijn geen persoonsgegevens indien deze geen informatie bevatten met behulp waarvan personen in hun maatschappelijke positie kunnen worden geraakt. Het gaat dan om zuivere *objectgegevens*. Hetzelfde geldt voor gegevens die onroerende zaken of andere registergoederen identificeren. Het feit dat deze zaken via een openbaar register zoals de kadastrale registratie tot een individuele natuurlijke persoon kunnen worden herleid, doet hieraan op zichzelf niet af.[22]

2.5 Verschillende typen gegevensuitwisseling

Bij het inventariseren van knelpunten in de gegevensuitwisseling en de verkenning van de mogelijkheden om deze met een kaderwet op te lossen, is het van belang vooraf te onderkennen

---

[19] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 46-47.

[20] Dat is bijvoorbeeld het geval wanneer de politie op grond van artikel 20 Wpg gegevens verstrekt aan de reclassering en de reclassering in het kader van een publiekrechtelijk samenwerkingsverband deze gegevens wil doorverstrekken aan de gemeente. Met het oog op een dergelijke situatie bepaalt artikel 22, zesde lid, Wbp dat het verbod om strafrechtelijke persoonsgegevens te verwerken, niet van toepassing is op verwerkingen door of ten behoeve van publiekrechtelijke samenwerkingsverbanden van verantwoordelijken of groepen van verantwoordelijken, indien de verwerking noodzakelijk is voor de uitvoering van de taak van deze verantwoordelijken of groepen van verantwoordelijken en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad (Kamerstukken II 2008-2009, 31 841, nr. 3, blz. 9).

[21] Zie bijvoorbeeld artikel 19.3 Wet milieubeheer en artikel 1:93 Wet op het financieel toezicht.

[22] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 47.

dat gegevensuitwisseling[23] verschillende verschijningsvormen kan hebben. Deze vormen laten zich categoriseren naar niveau en doel van uitwisseling, naar vorm van verwerking, naar de aard en frequentie van de uitwisseling, naar de vraag of van unilaterale, bilaterale dan wel multilaterale verstrekking sprake is, naar herkomst en – tot slot - naar de adressant van de gegevens.

Als het gaat om het *niveau en doel van gegevensuitwisseling*, kan onderscheid worden gemaakt tussen de volgende niveaus:

1. *Strategisch.* Het gaat hierbij om verwerking van gegevens, veelal van statistische aard, met het oog op het signaleren van trends en ontwikkelingen. Hiervoor worden in beginsel geen persoonsgegevens gebruikt.
2. *Tactisch.* Het gaat hierbij om verwerking van gegevens om tactische analyses te maken die uitmonden in mogelijke interventiestrategieën. Voorbeelden hiervan op het bredere terrein van criminaliteitsbestrijding en handhaving zijn de Bestuurlijke Criminaliteitsbeeldanalyses (BCBA's) die de RIEC's opstellen[24], en de gebiedsscans die de Omgevingsdiensten uitvoeren. Voor het opstellen van dergelijke analyses kan het noodzakelijk zijn ook persoonsgegevens te gebruiken. Daarbij kunnen zo mogelijk vormen van pseudonimisering of anonimisering worden toegepast.[25]
3. *Operationeel/zaakgericht.* Het gaat hierbij om gegevensuitwisseling in een concrete casus met als doel het verkrijgen van een goede informatiepositie op basis waarvan gezamenlijk kan worden bezien welke aanpak het meest effectief is. Voorbeelden hiervan zijn de gegevensuitwisseling binnen het FEC voor het opstellen van adviezen aan de FEC-partners voor het uitvoeren van bepaalde interventies[26] en de inkomens- en vermogensrapporten van de iCOV[27]. Het opstellen van dergelijke casusanalyses brengt uit de aard der zaak mee dat persoonsgegevens worden verwerkt.

De *vorm van verwerking* kan op de volgende aspecten betrekking hebben:

1. *Handmatig*. Te denken valt aan schriftelijke en mondelinge gegevensuitwisseling tijdens zgn. informatietafels of –pleinen in samenwerkingsverbanden. Er wordt hierbij geen gebruik gemaakt van ICT-voorzieningen.
2. *Geautomatiseerd*. Binnen samenwerkingsverbanden wordt op zeer verschillende manieren gebruik gemaakt van ICT-voorzieningen. In sommige gevallen is het gebruik van ICT slechts ondersteunend aan het primaire proces. Denk aan (beveiligde) systemen om de gegevensuitwisseling zorgvuldig te ontvangen en door te zenden en eventueel op maat vorm te kunnen geven. Dergelijke systemen zijn het "Colleges Collaboration Tool" (CoCoTo) van het FEC en het RIEC-IS van de RIEC's[28]. Bij deze systemen vervult het secretariaat van de samenwerking nog een belangrijke handmatige rol bij het verdelen en uitzetten van de gegevens. Dat is al weer anders bij geautomatiseerde kruispuntbanken waarbij gegevens op basis van een informatie- en autorisatiemodel geheel automatisch van bronhouder naar eindgebruiker gaan. Voorbeelden hiervan zijn Inspectieview Bedrijven en Inspectieview Milieu van de Inspectie Transport en Leefomgeving[29] en Suwi-inkijk. Tot slot zijn er samenwerkingsverbanden waar ICT-toepassingen centraal staan en voor een groot deel het

[23] Onder gegevensuitwisseling wordt hier in termen van de Wbp verstaan: de verstrekking van gegevens aan het samenwerkingsverband en de verdere verwerking van die gegevens binnen het samenwerkingsverband.
[24] Zie: http://www.riec.nl/instrumenten/bcba.
[25] Bij pseudonimisering wordt een identificerend gegeven vervangen door een ander identificerend gegeven. Bij anonimisering worden gegevens omgezet naar een vorm die identificatie niet langer mogelijk maakt.
[26] Zie het FEC-jaarverslag 2012-2014, voor het jaar 2014, blz. 9 (http://www.fec-partners.nl/media/76/42/705631/123/fec-jaarverlag_2012_-_2014_voor_het_jaar_2012.pdf).
[27] Zie Convenant iCOV 2013, Stcrt. 2013, 24607 (https://zoek.officielebekendmakingen.nl/stcrt-2013-24607.html). .
[28] Zie het jaarverslag 2012 van het LIEC, blz. 28 (http://www.liec.nl/doc/130136_RIEC-LIEC-Jaarverslag_web.pdf).
[29] Zie http://www.informatieuitwisselingmilieu.nl/pagina.php?id=3. Inmiddels is bij Inspectieview Milieu en Inspectieview Bedrijven voorzien in de mogelijkheid van een bulkbevraging. Analisten kunnen grote hoeveelheden gegevens opvragen om risico-analyses op te stellen.

primair proces beslaan. Hierbij kan worden gedacht aan gegevensuitwisseling door koppeling van bestanden van verschillende partners om met behulp van geavanceerde software bepaalde patronen te ontdekken (“datamining”)[30], gerichte bevragingen in databestanden van verschillende partners om bepaalde profielen vast te stellen (“profiling”). Een voorbeeld van dergelijke verwerkingen zijn verwerkingen met behulp van het Systeem Risico Indicatie (SyRI).[31]

Als het gaat om de *aard en frequentie van de uitwisseling*, kan zowel worden gedacht aan verstrekking op ad-hoc-basis ten behoeve van een bepaalde casus als aan gegevensuitwisseling van structurele aard. Bij het laatste valt te denken aan het maandelijks aan elkaar rapporteren van controles in een bepaald gebied en aan bepaalde producten die periodiek kunnen worden geleverd, zoals de iCOV-rapportage Inkomen en Vermogen.

Bij gegevensuitwisseling kan het gaan om zowel *unilaterale, bilaterale als multilaterale verstrekking van gegevens*. Bij unilaterale verstrekking is sprake van verstrekking door één partij aan één andere partij, bij bilaterale verstrekking van verstrekking door twee partijen over en weer en bij multilaterale verstrekking van verstrekking door en aan meer dan twee partijen.

De herkomst van de gegevens kan divers zijn. Een belangrijke, zo niet belangrijkste bron van de gegevens zal bij samenwerkingsverbanden uiteraard gelegen zijn in verstrekking door de deelnemers zelf. De samenwerking zal immers mede gestoeld zijn op de gedachte dat de deelnemers over gegevens beschikken die voor de andere deelnemers met het oog op het doel van het samenwerkingsverband van belang zijn. De gegevens kunnen echter ook een andere herkomst hebben. Daarbij kan worden gedacht aan gegevens uit openbare registers, gegevens uit andere openbare bronnen, gegevens uit registraties met authentieke gegevens, zoals de Basisregistratie personen, en gegevens die van bedrijfsinformatiebureaus als Dunn & Bradstreet afkomstig zijn.[32]

Tot slot de *adressant van de gegevens*. Bij samenwerkingsverbanden kan de gegevensuitwisseling in de eerste plaats bestaan uit directe verstrekking van gegevens aan één of meer andere partners in het verband, zonder dat deze gegevens in een apart bestand worden opgeslagen.[33] Voor deze vorm van gegevensuitwisseling zijn alleen de wettelijke regelingen van belang die voor de betrokken partijen gelden voor het verstrekken van gegevens aan het samenwerkingsverband, voor de politie de Wpg, voor het OM de Wjsg en voor de overige betrokken partners de Wbp (tenzij voor hen ook een bijzondere wet geldt). De gegevensuitwisseling kan ook bestaan uit verstrekking aan het samenwerkingsverband zelf, waarbij een organisatie die het verband ondersteunt, de verstrekte gegevens verwerkt tot specifieke informatieproducten als een casusanalyse, een gebiedsscan of profielen van bepaalde personen of bedrijven. Deze informatieproducten worden dan vervolgens weer ter beschikking gesteld van de deelnemers aan het samenwerkingsverband. De verwerking van gegevens tot dergelijke informatieproducten valt onder de Wbp. Zo’n verwerking zal in beginsel moeten worden aangemeld bij het College bescherming persoonsgegevens (art. 27 Wbp e.v.).

2.6 Belang van zorgvuldigheid bij gegevensuitwisseling

Bij een verkenning naar een kaderwet gegevensuitwisseling kan het niet alleen gaan om het verkennen van mogelijkheden om knelpunten weg te nemen die op dit moment met betrekking tot

[30] Bij deze vorm van gegevensverwerking doet de computer in feite zelf het werk. Mits de te verwerken data voldoende gestructureerd worden aangeboden, kunnen bepaalde computertools zelf uit deze data mogelijk relevante patronen halen. Daarmee kunnen modellen worden gemaakt waarmee niet alleen actuele risico’s in beeld kunnen worden gebracht, maar ook voorspellingen doen omtrent risico’s die zich mogelijk in de toekomst gaan voordoen (“predictive modelling”).
[31] Zie artikel 65 van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi).
[32] Vgl. artikel 7 Protocol gegevensverwerking iCOV Productie 2013, Stcrt. 2013, 24608.
[33] Zo worden in het Maritiem Informatie Knooppunt van de Kustwacht, waarin o.a. de politie, de Koninklijke marechaussee en de douane samenwerken, wel gegevens uitgewisseld, maar is er geen eigen bestand.

het uitwisselen van gegevens bestaan. Integendeel, een verbetering van de mogelijkheden tot gegevensuitwisseling die uit het wegnemen van deze knelpunten voortvloeit, schept een navenant grotere verantwoordelijkheid voor een zorgvuldige inrichting van het proces van gegevensuitwisseling. Anders gezegd: er zal een goede balans moeten worden gevonden tussen enerzijds de met een kaderwet beoogde verbetering van de mogelijkheden van gegevensuitwisseling en anderzijds de behoefte aan zorgvuldigheid bij die uitwisseling. Beide kunnen hand in hand gaan, als een kaderwet niet alleen knelpunten wegneemt, maar ook de nodige waarborgen voor een zorgvuldige gegevensverwerking bevat. Zo'n kaderwet kan dan ook een nieuwe impuls geven aan een zorgvuldige omgang met gegevens in de al bestaande praktijk van gegevensuitwisseling.

Dat bij iedere vorm van gegevensverwerking zorgvuldigheid voorop dient te staan, is op zich niets nieuws. De Wbp schrijft in artikel 6 nu al voor dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Waar het bij een verruiming van mogelijkheden van gegevensuitwisseling in samenwerkingsverbanden evenwel om gaat, is dat het principe van een zorgvuldige omgang met persoonsgegevens nog meer dan nu een algemeen erkende en aanvaarde praktische toetssteen bij de inrichting van deze gegevensuitwisseling zou kunnen vormen.

Zo'n toetssteen zou uiteraard in de eerste plaats gestoeld kunnen worden op een aantal bestaande waarborgen, zoals het principe van doelbinding, het noodzakelijkheidsvereiste en de beginselen van proportionaliteit en subsidiariteit. Dergelijke waarborgen vloeien al uit internationale verdragen, EU-richtlijnen en de daarop gebaseerde nationale wetten ter bescherming van persoonsgegevens voort. Wil het principe van een zorgvuldige omgang met persoonsgegevens in samenwerkingsverbanden een voldoende praktische toetssteen kunnen vormen, dan is het wenselijk dat een eventuele kaderwet een aantal aanvullende, meer specifieke waarborgen bevat. Te denken valt aan waarborgen met betrekking tot onder meer het koppelen van gegevensbestanden, de duiding van de kwaliteit van de gegevens en het uitvoeren van een "Privacy Impact Assessment". Een uitgebreidere uiteenzetting van mogelijke waarborgen is hierna in § 4.7 te vinden.

Het begrip "zorgvuldigheid", uitgewerkt in een aantal waarborgen, zou aldus het centrale ijkpunt bij iedere vorm en fase van gegevensverwerking in samenwerkingsverbanden moeten zijn. Dit impliceert dat bij de afweging wat bij gegevensverwerking wel en niet kan, dit begrip "zorgvuldigheid" telkens een leidende rol dient te vervullen. De eis van zorgvuldigheid brengt ook mee dat de uitkomsten van deze afwegingen en de daarbij gebruikte argumenten zo transparant mogelijk zijn.

Het vastleggen van een aantal waarborgen met betrekking tot een zorgvuldige gegevensuitwisseling in een kaderwet biedt niet alleen houvast voor partijen bij de inrichting van de processen waarin zij gegevens uitwisselen. Dergelijke waarborgen geven ook een handvat voor degenen van wie persoonsgegevens worden uitgewisseld. Met een verwijzing naar deze waarborgen kunnen zij immers, zo nodig, betwisten dat van een zorgvuldige gegevensuitwisseling sprake is. Het vastleggen van deze waarborgen in een kaderwet vergroot aldus de transparantie en daarmee de verantwoordelijkheid en aansprakelijkheid ("accountability") van de partijen in het samenwerkingsverband voor een zorgvuldige gegevensuitwisseling.

2.7 Betere gegevensuitwisseling: zaak van meer dan wetgeving alleen

Verbetering van de gegevensuitwisseling in samenwerkingsverbanden is een ambitie die niet alleen met een eventuele kaderwet kan worden gerealiseerd. Daarvoor is ook nodig dat partijen bereid zijn tot samenwerking en het delen van gegevens, daartoe de nodige organisatorische voorzieningen treffen en een adequate (technische) infrastructuur bouwen.

De bereidheid tot samenwerking hangt in de praktijk meestal af van de vraag of betrokken partijen belang in samenwerking zien. Vaak is het belang daarvan evident en soms is de samenwerking zelfs verankerd in wetgeving.[34] Intussen dringt wel steeds meer het besef bij overheidsorganisaties door dat het belang van samenwerking niet uitsluitend gelegen hoeft te zijn in een specifiek belang dat een individuele organisatie bij een eigen goede taakuitvoering heeft, maar dat samenwerking ook een breder, overkoepelend publiek belang kan en mag dienen. Als organisaties dat niet al uit zichzelf zijn gaan beseffen, is het wel de publieke opinie die daartoe een stimulans geeft. Zoals ook al in § 2.1 naar voren kwam, verwachten burgers en bedrijven immers in toenemende mate dat de overheid als één georganiseerd geheel optreedt.

Een en ander neemt niet weg dat samenwerking waar dat mogelijk en zelfs nodig zou zijn, niet steeds vanzelfsprekend is. Het komt nog voor dat cultuurverschillen en verkokerd denken samenwerking in de weg staan.[35] Hier ligt vooral een bestuurlijke opgave om deze drempels tot samenwerking te slechten. Een kaderwet gegevensuitwisseling kan in dit verband helpen, omdat het niet langer mogelijk is zich te verschuilen achter het argument dat bepaalde wettelijke voorschriften het uitwisselen van gegevens belemmeren en daarmee de mogelijkheden tot samenwerking beperken.

De bereidheid tot het uitwisselen van gegevens zal ook zijn ingegeven door het belang dat men daarbij heeft. Het directe belang bij de verstrekking van gegevens zal doorgaans bij de ontvangende partij liggen. Deze zal immers mede op basis van de ontvangen informatie een analyse kunnen uitvoeren, een interventie kunnen plegen dan wel daarop een andere handeling kunnen baseren. Doch ook de verstrekkende partij kan indirect belang bij de verstrekking hebben. Zo kan verstrekking van gegevens door de politie aan een gemeente ertoe leiden dat de gemeente een maatregel neemt die een bepaalde vorm van criminaliteit voorkomt, zodat de politie niet zelf hoeft op te treden. In dit licht bezien hoeft samenwerking niet te betekenen dat er altijd van een bilaterale of multilaterale verstrekking van gegevens sprake moet zijn; ook een unilaterale verstrekking van gegevens kan de belangen van beide betrokken partijen dienen.

In het geval dat er bij een partij geen taken of belangen zijn aan te wijzen die tot verstrekking van gegevens aan een andere partij nopen, kan een goede taakuitvoering door die andere partij toch aanleiding tot verstrekking zijn. Uitgaande van een kaderwet die in zo'n geval verstrekking mogelijk maakt, is ook dan vooral sprake van een bestuurlijke opgave om deze mogelijkheid te benutten door daarover afspraken te maken. Als deze opgave niet wordt opgepakt, resteert slechts het middel van een wettelijke verplichting tot verstrekking.

Om de gegevensuitwisseling in een samenwerkingsverband goed te laten verlopen, dient ook een aantal organisatorische voorzieningen te worden getroffen. Van essentieel belang is dat de eigen informatiehuishouding op orde is: weten de deelnemende organisaties welke gegevens zij in huis hebben en hebben zij de verwerking van deze gegevens in goede procesbeschrijvingen vastgelegd, waaruit helder naar voren komt op welke wettelijke grondslagen deze verwerking plaatsvindt en wie geautoriseerd is om toegang tot welke (categorieën van) gegevens te hebben? Slechts vanuit een adequaat beeld van de eigen informatiehuishouding kunnen organisaties vervolgens de vraag onder ogen zien welke (categorieën van) gegevens noodzakelijk zijn voor een samen op te richten samenwerkingsverband en zij om die reden willen gaan uitwisselen.

Voordat tot gegevensuitwisseling wordt overgegaan, dienen betrokken partijen daarover goede afspraken te maken. Afspraken over het doel van de samenwerking, de aansturing van het samenwerkingsverband en de hoofdlijnen van de gegevensuitwisseling worden vaak – zie ook § 2.2 - in een convenant vastgelegd. Afspraken over de gegevensuitwisseling worden dan meestal

---

[34] Een voorbeeld daarvan is de samenwerking tussen het UWV, de SVB en de gemeenten bij de uitvoering van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi) enige andere wetten. Zie daarvoor art. 9 Wet Suwi.

[35] Zie in dit verband ook: A.J.C. de Moor-van Vugt, Gegevensuitwisseling door Toezichthouders; onderzoek uitgevoerd in opdracht van het WODC, 2012, blz. 56.

uitgewerkt in een informatie- of privacyprotocol. Daarbij is van belang een heldere beschrijving te geven van de inrichting van de gegevensuitwisseling: welke partijen wisselen welke gegevens in welk proces uit om tot welk resultaat of product te komen? Bij de inrichting daarvan moet uiteraard acht worden geslagen op de vorm en mate waarin hiervoor relevante regelgeving de gegevensuitwisseling toelaten.

Ter ondersteuning van het samenwerkingsverband wordt vaak een bureau in het leven geroepen die voor de feitelijke gegevensuitwisseling zorgdraagt, analyses en rapportages opstelt en adviezen geeft. Afhankelijk van de gemaakte afspraken beheert zo'n organisatie vaak ook een informatiesysteem waarin de uitgewisselde gegevens worden verwerkt. Een heldere beschrijving van de inrichting van de gegevensuitwisseling is niet alleen nodig om die uitwisseling goed te laten verlopen, maar ook een randvoorwaarde voor het opzetten van een dergelijk informatiesysteem. Daarmee wordt voorkomen dat een systeem wordt ontwikkeld dat naderhand gegevens blijkt te verwerken op een wijze die niet strookt met de geldende regelgeving, en dan tegen wellicht hoge kosten moet worden aangepast.

2.8 Relevante andere ontwikkelingen

Bij deze verkenning is mede acht geslagen op verschillende ontwikkelingen die betrekking hebben op gegevensverwerking in het algemeen.

Een eerste ontwikkeling die hier wordt genoemd, betreft het onderzoek dat in het verleden naar gegevensuitwisseling door toezichthouders is verricht. In 2008 heeft een interdepartementale werkgroep herijking toezichtregelgeving onderzocht wat de mogelijke juridische belemmeringen zijn voor de voortzetting en intensivering van de samenwerking tussen de rijksinspecties en welke mogelijkheden er zijn deze belemmeringen weg te nemen. De werkgroep kwam tot de conclusie dat een algemene wettelijke regeling voor de informatie-uitwisseling tussen inspecties die een gelijk regime voor alle inspecties zou creëren, niet goed mogelijk en niet wenselijk is. De werkgroep voerde daartoe aan dat er immers sprake is van nogal uiteenlopende toezichthoudende organen, die gegevens van allerlei aard uitwisselen waarvoor diverse regimes gelden. Het zou volgens de werkgroep zeer de vraag zijn of het zou lukken deze regimes in een overkoepelende regeling onder te brengen. Bovendien zou een algemeen geldende doelomschrijving voor de overdracht van gegevens voor inspectiedoeleinden op problemen kunnen stuiten in relatie tot de eis uit artikel 6 van de Europese privacyrichtlijn dat het doel van de verwerking van persoonsgegevens welbepaald moet zijn.[36] Het toenmalige kabinet nam deze conclusie over.[37] Bij de behandeling van het kabinetsstandpunt inzake het advies van de Commissie Brouwer-Korf en de evaluatie van de Wbp is op aandringen van de Tweede Kamer toegezegd de mogelijkheid van een dergelijke algemene regeling toch te bezien.[38] Het toenmalige kabinet heeft in dat verband gewezen op de mogelijkheid van een algemene wettelijke bepaling die inhoudt dat gegevens in het kader van een structurele samenwerking kunnen worden uitgewisseld, mits de afspraken tot samenwerking op een wettelijk voor te schrijven wijze zijn bekendgemaakt.[39] De toezegging van het kabinet heeft geleid tot een onderzoek in opdracht van het WODC naar gegevensuitwisseling door toezichthouders. Dat onderzoek heeft geleid tot een rapport waarin wordt aanbevolen om – mede ten behoeve van een vereenvoudiging en verduidelijking van de eis van doelbinding – de huidige Wbp om te vormen tot een brede kaderwet, eventueel met nadere uitwerking in sectorale wetgeving. Ook bevat het rapport aanbevelingen voor het gebruik van convenanten ten behoeve van structurele gegevensverstrekking in publiekrechtelijke samenwerkingsverbanden.[40] Het kabinet heeft in reactie op dat rapport zich op het standpunt gesteld dat de herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens (zie hierna) een goed moment is voor een meer algemene bezinning op het huidige nationale kader, waarin

[36] Rapport van de werkgroep herijking toezichtregelgeving, 2008, § 4.2.2.
[37] Kamerstukken II 2008-2009, 31700 VI, nr. 70.
[38] Kamerstukken II 2009-2010, 31051, nr. 7, blz. 19.
[39] Kamerstukken II 2008-2009, 31700 VI, nr. 118, blz. 9.
[40] De Moor-van Vugt, a.w., blz. xiv.

het zwaartepunt ligt bij de sectorale wetgeving.[41] Al deze aspecten zullen in deze verkenning moeten worden meegewogen, meer in het bijzonder bij een bespreking van de mogelijke contouren van een eventuele kaderwet (zie § 4).

De werkgroep herijking toezichtregelgeving heeft destijds in haar rapport ook een serie modelbepalingen opgenomen voor gegevensverstrekking door in de desbetreffende wet te noemen bestuursorganen en toezichthouders aan andere bestuursorganen die deze voor de uitvoering van hun taak behoeven.[42] Deze modelbepalingen zijn naderhand ook opgenomen in de Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens die het toenmalige kabinet heeft meegezonden met de Notitie privacybeleid.[43] Deze modelbepalingen dienen te worden gebruikt, indien het noodzakelijk is dat op structurele basis wordt voorzien in de onderlinge verstrekking van persoonsgegevens tussen bestuursorganen of toezichthouders, terwijl geldende geheimhoudingsbepalingen daaraan in de weg staan. Voor dat geval schrijven de Aanwijzingen voor de regelgeving voor dat op het niveau van de formele wet wordt voorzien in een uitdrukkelijke regeling van de gegevensverstrekking, met inbegrip van de vaststelling van het doel van de gegevensverstrekking.[44]

Een ontwikkeling waarmee ook rekening moet worden gehouden, is de inwerkingtreding op 1 januari 2014 van de Wet tot wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi) en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Stb. 2013, 405). Deze wet introduceert nieuwe mogelijkheden van gegevensuitwisseling voor de aanpak van fraude op het terrein van sociale zekerheid en inkomensafhankelijke regelingen, belastingen, premies en arbeidswetten. Zij geeft tevens een wettelijke verankering van het instrument Systeem Risico Indicatie (SyRI). SyRI omvat de technische infrastructuur en bijbehorende procedures om in een beveiligde omgeving op een zorgvuldige manier gepseudonimiseerde data te koppelen en te analyseren, zodat op basis daarvan risicomeldingen met betrekking tot mogelijke fraude kunnen worden gegenereerd. SyRI kan worden gebruikt door samenwerkingsverbanden waaraan in ieder geval de gemeenten, de Belastingdienst, het UWV, de SVB en de Inspectie SZW deelnemen. In zekere zin kan deze wet tot wijziging van de Wet Suwi worden gezien als inspiratiebron voor de onderhavige verkenning naar een kaderwet gegevensuitwisseling. Immers, verschillende elementen van deze wijzigingswet en het daarop gebaseerde uitvoeringsbesluit[45] zijn in enigerlei vorm terug te vinden in § 4 van deze notitie, waarin de contouren van een mogelijke kaderwet gegevensuitwisseling worden beschreven. Te denken valt aan de ruime doelbinding, de toepasselijkheid op meerdere samenwerkingsverbanden en een aantal waarborgen, zoals de noodzakelijke expliciete toets aan de beginselen van proportionaliteit en subsidiariteit.

Een ander relevant traject wordt gevormd door de beleidsvisie van het kabinet met richtlijnen voor het zorgvuldig omgaan met persoonsgegevens in de gemeentelijke praktijk in het kader van de zgn. drie decentralisaties. Bij het opstellen van die visie is uitgegaan van het belang dat gemeenten op een soepele manier informatie over burgers kunnen opvragen en uitwisselen, zonder dat er nodeloos of overmatig gegevens worden opgevraagd, gedeeld of anderszins verwerkt. Bij de totstandkoming van die visie is vooralsnog geconcludeerd dat er voor het mogelijk maken van de gewenste gegevensdeling geen noodzaak is voor een nieuw juridisch kader voor gegevensverwerking en privacy in het sociaal domein.[46] Dit impliceert dat de onderhavige

---

[41] Kamerstukken II 2012-2013, 32761, nr. 43.
[42] Zie Rapport van de werkgroep herijking toezichtregelgeving, 2008, § 4.2.3.
[43] Kamerstukken II 2010-2011, 32761, nr. 1.
[44] Aanwijzingen voor de regelgeving, nr. 162b.
[45] Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisseling en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI (Stb. 320).
[46] Kamerstukken II 2013-2014, 32761, nr. 62, blz. 1.

verkenning, voor zover zij al op een breder terrein dan fraudebestrijding betrekking heeft, in ieder geval niet het sociaal domein omvat waarop de drie decentralisaties zich afspelen.

Deze verkenning vertoont ook samenhang met het rapport "Dienstbaar en transparant" van het project SGO-3. In dat rapport adviseert de stuurgroep SGO-3 een programma te starten voor het ontwikkelen van een kaderwet die de hanteerbaarheid van de huidige privacywet- en regelgeving verbetert. De stuurgroep adviseert om dit traject af te stemmen met de onderhavige verkenning naar de mogelijkheden van een kaderwet voor de gegevensuitwisseling ten behoeve van de fraudebestrijding.[47]

Voor deze verkenning is ook relevant dat op dit moment in Brussel onderhandelingen plaatsvinden over voorstellen van de Europese Commissie voor een Algemene verordening gegevensbescherming[48] en een Richtlijn gegevensbescherming opsporing en vervolging[49]. De beoogde verordening moet de Europese privacyrichtlijn uit 1995[50] vervangen. Als verordening zal zij directe werking in Nederland hebben en tot gevolg hebben dat de Wet bescherming persoonsgegevens en bepalingen ter bescherming van persoonsgegevens in specifieke wetten overbodig worden dan wel aanpassing behoeven. De beoogde richtlijn gegevensbescherming opsporing en vervolging zal geen directe werking hebben en moeten worden omgezet in nationale wetgeving. Als gevolg daarvan zullen de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens aanpassing behoeven. Beide voorstellen van de Europese Commissie bevatten geen bepalingen die specifiek op gegevensuitwisseling in samenwerkingsverbanden betrekking hebben. Dat neemt niet weg dat bij de verdere voorbereiding van een eventuele kaderwet met de onderhandelingen over de komende verordening en richtlijn rekening moet worden gehouden. In § 4.15 wordt daaraan al een eerste beschouwing gewijd.

Een andere ontwikkeling waarop in deze verkenning wordt gewezen, is de evaluatie van de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze evaluatie heeft geleid tot een brief van de Minister van Veiligheid en Justitie van 23 juni 2014 aan de Tweede Kamer, waarin hij een perspectief schetst op de toekomstige omgang met politiële, justitiële en strafvorderlijke gegevens. In de brief wordt de conclusie getrokken dat deze wetten moeten worden gemoderniseerd, waarbij de verschillende regimes die van toepassing zijn op politiële, justitiële en strafvorderlijke gegevens, moeten worden geharmoniseerd, het gebruik van gegevens en niet de bewaartermijnen het uitgangspunt van de nieuwe regelgeving moet zijn en het toezicht op het gebruik en de verstrekking van gegevens moet worden versterkt. Deze modernisering van de regelgeving en de uitvoering is volgens de Minister ambitieus en zal de nodige tijd kosten.[51] Met betrekking tot samenwerkingsverbanden merkt hij in de brief op dat in verschillende verbanden, waarin ook politiële, justitiële en strafvorderlijke gegevens worden uitgewisseld, in toenemende mate met convenanten en privacyprotocollen wordt gewerkt. Hij stelt daarbij dat hij deze werkwijze krachtig verder zal bevorderen.[52] Bij de voorbereiding van een eventuele kaderwet gegevensuitwisseling zal met dit moderniseringstraject rekening moeten worden gehouden en zal ook het belang van convenanten en privacyprotocollen moeten worden meegewogen.

Tot slot valt nog te wijzen op de verkenning naar een aantal scenario's om de informatiepositie van bestuursorganen bij de toepassing van de Wet bevordering integriteitsbeoordelingen openbaar

---

[47] Eindrapport project SGO-3 "Versnelde effectieve inzet van basisregistraties", mei 2014, blz. 45 (http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2014/05/22/de-basisregistraties-van-de-nederlandse-overheid-dienstbaar-en-transparant.html).

[48] Zie voorstel van de Europese Commissie van 25 januari 2012, COM(2012)11.

[49] Zie voorstel van de Europese Commissie van 25 januari 2012, COM(2012)10.

[50] Richtlijn 95/46/EG van het Europees parlement en de Raad van 24 oktober 1995, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Pb L 281.

[51] Kamerstukken II 2013-2014, 33842, nr. 2, blz. 1-2.

[52] Idem, blz. 8.

bestuur (Wet Bibob) te verbeteren. Deze verkenning is toegezegd tijdens de behandeling van het voorstel van de Evaluatie- en uitbreidingswet Bibob in de Eerste Kamer.[53] Eén van deze scenario's gaat uit van een versterking van de rol van de RIEC's bij de uitvoering van de Wet Bibob. Zo'n scenario kan relevant zijn bij de verdere uitwerking van een eventuele kaderwet. Uiteraard hangt de relevantie daarvan ook af van het kabinetsstandpunt dat naar aanleiding van die verkenning zal worden uitgebracht.

[53] Kamerstukken I 2012-2013, 32676 H, blz. 3,

3. Knelpunten

3.1 Inleiding

In § 1 van deze verkenning is naar voren gebracht dat de werkgroep haar verkenning van knelpunten bij de gegevensuitwisseling in samenwerkingsverbanden gebaseerd heeft op bestaande ervaringen, een brainstormsessie met experts, de bestudering van een viertal casussen en van literatuur, officiële publicaties en websites. De werkgroep merkt in dit verband op dat zij weliswaar primair aandacht heeft besteed aan gegevensuitwisseling ten behoeve van de fraudebestrijding, maar zich niet tot dat terrein heeft beperkt. Dat heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uitsluitend fraudebestrijding bezighouden (zie § 2.3). De tweede reden is dat knelpunten bij gegevensuitwisseling ten behoeve van andere doeleinden evenzeer van belang kunnen zijn, zeker in het geval voor een kaderwet met een bredere reikwijdte dan alleen fraudebestrijding zou worden gekozen (zie nader § 4.2).

3.2 Verschillende wettelijke kaders

Gegevensverwerking heeft altijd een centrale plaats gehad bij de interne werkprocessen van veel overheidsorganisaties en in de verhouding overheid-burger. Gegevensverwerking is immers een belangrijk onderdeel van en dienstbaar aan de opgedragen taak van praktisch iedere overheidsinstelling. Iedere overheidsinstelling heeft zijn eigen taak en oefent een eigen gegevenshuishouding uit bij de uitvoering van die taak. Zolang de gegevensverwerking plaats vindt binnen het kader van de eigen taak, wordt de bevoegdheid tot dergelijke gegevensverwerking geacht op te gaan in de algemene taakomschrijving nu die dienstig is aan die taakinvulling en daarvoor noodzakelijk is. In deze situatie is het opnemen van bepalingen rond gegevensverwerking beperkt tot het opnemen van informatieverplichtingen voor burgers die met de betrokken overheidsinstelling te maken hebben. Ook is meestal sprake van een geheimhoudingsbepaling voor de betrokken overheidsdienst zodat de burger of het bedrijf erop kan vertrouwen dat zijn gegevens in veilige handen zijn (zie ook § 3.5). Daarmee is sprake van geïsoleerde, gesloten gegevenshuishoudingen per domein of zelfs per overheidsdienst.

Pas wanneer sprake is van een behoefte bij de ene overheidsdienst aan gegevens waarover een andere overheidsdienst beschikt en dus aan het uitwisselen van gegevens tussen overheidsdiensten, ontstaat de noodzaak een dergelijke uitwisseling van gegevens juridisch in te kaderen c.q. van een adequate juridische grondslag te voorzien. De bevoegdheid gegevens uit te wisselen met een ander valt in beginsel buiten de taakomschrijving van de betrokken overheidsdienst, zoals die door de wetgever in de vorm van taken en bevoegdheden aan die dienst is geattribueerd. De bevoegdheid gegevens te delen met een andere overheidsdienst dient derhalve expliciet in het leven te worden geroepen. Inmiddels is er dan ook een groot aantal bepalingen tot stand gekomen op grond waarvan de ene overheidsdienst gegevens verstrekt aan de andere overheidsdienst. Voor ieder rechtsgebied dan wel iedere overheidsinstelling is dit overigens op eigen wijze geregeld, passend binnen de regelgeving die geldt voor dat rechtsgebied of die instelling.

Anders gezegd: regelingen met betrekking tot verwerking van gegevens hebben uit hun aard primair een “verticaal” karakter: zij regelen de gegevensverwerking *binnen* de desbetreffende sector. Gegevensuitwisseling in samenwerkingsverbanden heeft echter een “horizontaal” karakter: zij heeft betrekking op gegevensverwerking *tussen* verschillende sectoren. Voor zover sectorspecifieke regelingen bepalingen bevatten over verstrekking aan derden, hebben deze bovendien meestal betrekking op bilaterale verstrekking en niet op verstrekking aan meerdere partijen tegelijk die in een samenwerkingsverband opereren.[54]

[54] Uitzonderingen hierop zijn o.a. te vinden in de artikel 20 Wet politiegegevens, artikel 28, tweede lid, onder d, Wet Bibob en artikel 64 Wet Suwi. Verder bevat ook de Wbp in artikel 22, zesde lid, een specifieke bepaling met betrekking tot verstrekking van strafrechtelijke gegevens door en ten behoeve van samenwerkingsverbanden.

Gelet op de specifieke context waarin overheidsorganisaties moeten opereren, is de systematiek van de bestaande wetgeving voor iedere individuele organisatie wellicht nog te begrijpen en te billijken. Deze systematiek van de wetgeving is voor samenwerkingsverbanden echter wel erg complex. Zo complex dat het ook voor deskundigen lastig is door de bomen het bos te zien. Het gaat dan nog niet eens zozeer om het grote aantal normen dat in acht moet worden genomen, maar meer nog om het feit dat die normen in relatie tot samenwerkingsverbanden in bepaalde gevallen niet goed te duiden zijn. Het kan dan bijvoorbeeld gaan om de vraag of en, zo ja, in hoeverre bepalingen die bilaterale verstrekking mogelijk maken, ook kunnen worden benut voor gegevensuitwisseling binnen het samenwerkingsverband.[55] De slagkracht van de samenwerking kan zodoende teloor gaan door de veelheid aan interpretaties van de bestaande, veelal sectorale regels en door wettelijke belemmeringen. Er bestaat onzekerheid over essentiële vragen als die of gegevensuitwisseling wel is geoorloofd in een concrete situatie en wat daarbij precies de randvoorwaarden zijn. Daardoor is in de praktijk gegevensuitwisseling niet steeds vanzelfsprekend, waar zij dat wel zou kunnen of zelfs moeten zijn. En dit belemmert een adequate aanpak.

De introductie van modelbepalingen over gegevensverstrekking (zie § 2.8) heeft in deze situatie onvoldoende verandering kunnen brengen. Deze modelbepalingen zijn bestemd voor situaties waarin sprake is van bilaterale dan wel multilaterale gegevensuitwisseling door in de wet bij naam te noemen partijen. Dit impliceert dat voor elk samenwerkingsverband een afzonderlijke wettelijke regeling moet worden gemaakt. De praktijk heeft evenwel behoefte aan een wettelijk kader waarbinnen meerdere samenwerkingsverbanden voor verschillende specifieke doelen kunnen worden opgericht. Zo'n kader zou voldoende ruimte moeten bieden voor maatwerk voor ieder afzonderlijk samenwerkingsverband. Aldus zou op een snellere wijze kunnen worden ingespeeld op de behoefte aan samenwerkingsverbanden dan met de modelbepalingen mogelijk is. Daar komt bij dat deze modelbepalingen niet een oplossing bieden voor alle knelpunten die hierna nog aan de orde komen.

Meer in het bijzonder bij verstrekking van strafrechtelijke gegevens aan samenwerkingsverbanden is bij de evaluatie van de Wpg en de Wjsg gebleken dat zich daarbij verschillende knelpunten voordoen. De belangrijkste knelpunten die in dit verband bij de evaluatie van de Wpg zijn genoemd, zijn onduidelijkheid over wanneer verstrekken begint, wat je mag verstrekken, de soms tegenstrijdige wettelijke kaders, de plaats en positie van convenanten en hoe het staat met de informationele privacy nadat verstrekt is.[56] De evaluatie van de Wjsg laat zien dat het bij samenwerkingsverbanden zelfs voor goed ingelichte betrokkenen vaak niet duidelijk is of gegevens nu via de Wpg, de Wjsg of zelfs via de Wbp moeten worden verwerkt. Daar komt bij dat, als gegevens onder de werking van zowel de Wjsg als de Wpg (lijken te) vallen, men voor verstrekking van gegevens aan samenwerkingsverbanden voor het ruimere regime van de Wpg kiest boven dat van de Wjsg.[57]

3.3 Rechtvaardigingsgronden

Uit de inventarisatie van de werkgroep volgt dat een knelpunt voor de gegevensuitwisseling binnen samenwerkingsverbanden onder meer is gelegen in de rechtvaardigingsgronden die de Wbp voor de verwerking van persoonsgegevens bevat.

---

[55] Zo merkte de Raad van State in zijn advies over het voorstel tot wijziging van de Wet op het financieel toezicht en enige andere wetten (Wijzigingswet financiële markten 2014) op dat toezichthouders toezichtvertrouwelijke informatie slechts mogen verstrekken in één-op-één relatie met in de wet genoemde partijen. Deze eis stond volgens de Raad in de weg aan hetgeen met het voorstel wordt beoogd, namelijk het mogelijk maken van informatie-uitwisseling binnen het FEC. De regering heeft de desbetreffende bepaling vervolgens zo aangepast dat de informatie slechts mag worden verstrekt als dat voor de ontvangende partij dienstig is voor de uitoefening van haar wettelijke taak (kamerstukken II 2012-2013, 33632, nr. 4, blz. 18-19).
[56] WODC, Glazen privacy. Knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg), 2013, blz. 89.
[57] WODC, Onderzoeksrapport Evaluatie Wet justitiële en strafvorderlijke gegevens, 2013, blz. 84, 91.

Persoonsgegevens mogen ingevolge artikel 7 Wbp alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer sprake is van "gerechtvaardigde doeleinden", valt af te leiden uit artikel 8 Wbp. Dat artikel bepaalt in een limitatieve opsomming van gronden wanneer de verwerking – dus ook het verzamelen - van persoonsgegevens gerechtvaardigd is. Dat is het geval wanneer de betrokkene uitdrukkelijk toestemming heeft verleend (a) of wanneer de verwerking noodzakelijk is ter uitvoering van een overeenkomst (b), ter nakoming van een wettelijke verplichting (c), ter vrijwaring van een vitaal belang van de betrokkene (d), voor de goede vervulling van een publiekrechtelijke taak door een bestuursorgaan (e) of ter behartiging van het gerechtvaardigde belang van de verantwoordelijke, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert (f).

Voor gegevensuitwisseling in samenwerkingsverbanden op het terrein van de fraudebestrijding geldt dat deze uiteraard niet afhankelijk kan zijn van toestemming van betrokkenen. Fraudeurs hebben er eerder belang bij dat hun gegevens niét worden uitgewisseld, als daardoor de kans groter wordt dat zij gepakt worden. Dat de gegevensuitwisseling noodzakelijk is ter uitvoering van een overeenkomst, zal zich bij dergelijke samenwerkingsverbanden ook niet voordoen. Op een wettelijke verplichting tot gegevensverstrekking kan veelal ook geen beroep worden gedaan.[58] Daarbij moet worden bedacht dat een eventuele bevoegdheid tot gegevensverstrekking nog geen wettelijke verplichting impliceert. Ook van een vitaal belang van betrokkenen zal geen sprake zijn. Zo resteren de gronden e en f.

Van deze twee gronden is voor samenwerkingsverbanden de grond, genoemd onder e, het meest relevant. Zij legitimeert de verstrekking van persoonsgegevens door een bestuursorgaan aan een ander bestuursorgaan, als deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het verstrekkende orgaan dan wel het orgaan waaraan de gegevens worden verstrekt. Zo'n verstrekking kan ook plaatsvinden in het kader van een samenwerkingsverband. Wel moet een multilaterale verstrekking in zo'n verband voor ieder van de afzonderlijke deelnemers kunnen worden gerechtvaardigd. Dat vloeit nu eenmaal uit de formulering van deze rechtvaardigingsgrond voort, waarin een samenwerkingsverband als zodanig immers niet voorkomt. Hetzelfde geldt voor bepalingen uit sectorale wetten die bilaterale verstrekking mogelijk maken (zie nader § 3.4). Een en ander impliceert dat voor gegevensverstrekking aan alle deelnemers van een samenwerkingsverband tegelijk of aan een ondersteunend bureau, als dat voor een effectief functioneren van het verband als geheel ten goede zou komen, vaak geen adequate grondslag bestaat. Een kaderwet zou deze belemmering kunnen wegnemen.

Kan aldus het vinden van een rechtvaardigingsgrond voor gegevensuitwisseling tussen bestuursorganen in een samenwerkingsverband al problemen opleveren, het ligt nog een slag lastiger, als aan een samenwerkingsverband ook private partijen – zie § 2.3 - deelnemen. Tenzij een sectorspecifieke wet voor dat geval gegevensverstrekking mogelijk maakt, zal de verstrekking uitsluitend kunnen worden gebaseerd op eerdergenoemde grond f. Een beroep op die grond brengt echter mee dat steeds een afweging voor het individuele geval moet worden gemaakt. Dat belemmert een structurele uitwisseling van gegevens. Als een eventuele kaderwet voor gegevensuitwisseling bij fraudebestrijding ook op uitwisseling met private partijen betrekking zou hebben, zou deze kaderwet die belemmering kunnen wegnemen.

3.4 Verenigbaarheidstoets

Aan de rechtvaardigingsgronden van artikel 8 voegt artikel 9 Wbp de algemene eis toe dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de

[58] Een uitzondering hierop wordt onder meer gevormd door artikel 64, derde lid, Wet Suwi, waarin de deelnemers aan een samenwerkingsverband worden verplicht elkaar de noodzakelijke gegevens te verstrekken. Andere voorbeelden zijn te vinden in artikel 29a Arbeidsomstandighedenwet, artikel 8:7 Arbeidstijdenwet en artikel 18p Wet minimumloon en minimumvakantiebijslag.

doeleinden waarvoor ze zijn verkregen (principe van doelbinding). Het doel van de gegevensuitwisseling in een samenwerkingsverband is in het algemeen een ander dan het doel waarvoor een deelnemer aan het verband de gegevens oorspronkelijk heeft verkregen. Dit brengt mee dat voor deze gegevensuitwisseling moet worden getoetst of zij al dan niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verkregen.[59]

De uitvoering van de verenigbaarheidstoets wordt in de praktijk als een lastige hindernis ervaren en zet om die reden bij tijd en wijle een juridische rem op de bereidheid om gegevens uit te wisselen.[60] Weliswaar geeft artikel 43 Wbp voor bepaalde doeleinden de mogelijkheid om af te wijken van het principe van doelbinding, maar uit de zeer casuïstische jurisprudentie over dit artikel kan worden afgeleid dat toepassing slechts is weggelegd voor uitzonderlijke gevallen en niet gebruikt kan worden als een grondslag voor permanente of anderszins structurele overdracht van gegevens.[61] Artikel 43 biedt daarmee voor samenwerkingsverbanden geen uitkomst.

Los van deze overweging dient aan het beginsel van doelbinding en daarmee aan de verenigbaarheidstoets ook grote waarde te worden toegekend. Aan beide kan ook in het licht van de Europese privacyregelgeving en de Nederlandse wetgeving geen afbreuk worden gedaan. Het is dan ook ondenkbaar dat een eventuele kaderwet de verenigbaarheidstoets terzijde zou kunnen schuiven. Overigens lijkt men in de praktijk soms een te krampachtige houding bij de uitvoering van de verenigbaarheidstoets in te nemen. Dat kan tot het achterwege laten van gegevensuitwisseling leiden, waar een goed uitgevoerde verenigbaarheidstoets wel ruimte voor zou kunnen geven. Waar op dit punt wetgeving geen uitkomst kan bieden, zou voorlichting dat wel kunnen.

Niet zonder belang is dat er mogelijk verandering komt in de omstandigheid dat de Europese privacyregelgeving weinig tot geen ruimte laat voor verdere verwerking van persoonsgegevens voor een doel dat niet verenigbaar is met het doel waarvoor zij zijn verzameld. Ingevolge artikel 6, vierde lid, van het voorstel voor een Algemene verordening gegevensbescherming is ingeval van onverenigbare doelen verdere verwerking toch mogelijk, mits deze verwerking haar rechtsgrondslag heeft in tenminste één van de gronden die dat artikel in het eerste lid, onder a tot en met e noemt. De gronden die in relatie tot samenwerkingsverbanden relevant zijn, zijn de gronden c en e. Het gaat om het geval dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting van de voor de verwerking verantwoordelijke (grond c) en het geval dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang (grond e). Indien een verenigbaarheidstoets tot de conclusie leidt dat van onverenigbare doelen sprake is, zal verdere verwerking onder de Algemene verordening gegevensbescherming toch mogelijk zijn, als daarvoor één van genoemde gronden kan worden aangevoerd.[62]

3.5 Geheimhoudingsplicht

De mate waarin gegevens binnen samenwerkingsverbanden kunnen worden uitgewisseld, wordt thans ook sterk bepaald door de bestaande geheimhoudingsplichten. Deze plichten zijn ingegeven met het oog op verschillende belangen. Daarbij kan het onder meer gaan om bescherming van

---

[59] Voor het toetsen of er sprake is van verenigbaar gebruik draagt het tweede lid van artikel 9 Wbp de volgende vijf criteria aan:

1. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen,
2. de aard van de gegevens,
3. de gevolgen van de beoogde verwerking voor de betrokkene,
4. de wijze waarop de gegevens zijn verkregen, en
5. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

[60] Zie in dit verband ook: De Moor-van Vugt, a.w., blz. 35, 59.

[61] Vgl. kamerstukken II 2008-2009, 29911, nr. 23, blz. 8. Zie ook HR 31 januari 2012 (LJN: BT7126, pag. 19) en de Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, 2010, blz. 68.

[62] Zie over de verhouding tot de regelgeving van de EU ook § 4.15.

private belangen (persoonlijke levenssfeer, bedrijfsgeheimen), bescherming van publieke belangen (veiligheid van de staat), bescherming van de bijzondere positie van bepaalde ambten (onschendbaarheid Koning) en de zorg voor de goede werking van het openbaar bestuur (mogelijkheid van intern beraad, geheimhouding van een bepaalde werkwijze, het belang van inspectie, toezicht en controle door bestuursorganen).[63]

Bij gegevensuitwisseling in samenwerkingsverbanden zijn de bescherming van private belangen en de zorg voor de goede werking van het openbaar bestuur het belangrijkst. De bescherming van private belangen is overigens niet alleen een belang van burgers en bedrijven, maar eveneens van de overheid zelf. De belangen lopen parallel, daar waar bescherming bijdraagt aan het beeld van de betrouwbare overheid. Burgers en bedrijven zullen immers eerder geneigd zijn gegevens af te staan aan de overheid als zij erop kunnen vertrouwen dat deze goed worden bewaakt en niet zomaar aan de openbaarheid of aan derden worden prijsgegeven. In die zin dient de bescherming van private belangen tevens het organisatiebelang en de goede werking van het openbaar bestuur. Anderzijds kan de bescherming van private belangen juist de goede werking van het openbaar bestuur belemmeren, als overheidsinstanties zich onderling beroepen op de geheimhoudingsplicht en om die reden niet tot uitwisseling van gegevens overgaan. Daarbij moet worden bedacht dat geheimhoudingsplichten in de regel in het leven zijn geroepen met het oog op een bepaald deelbelang binnen het openbaar bestuur, zoals de correcte belastingheffing of de bewaking van de soliditeit van banken. De geheimhoudingsplicht heeft aldus meer kanten.[64]

Een algemene geheimhoudingsplicht is opgenomen in de Algemene wet bestuursrecht (Awb). Artikel 2:5 Awb bepaalt dat een ieder die betrokken is bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, verplicht is tot geheimhouding van die gegevens. Deze geheimhoudingsplicht is aanvullend: zij geldt niet voor wie reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt. Verder wijkt deze plicht voor een wettelijk voorschrift dat tot mededeling verplicht, terwijl ook uit de taakuitoefening een noodzaak tot mededeling kan voortvloeien. Tot de gegevens met een vertrouwelijk karakter kunnen onder meer bedrijfs- en fabricagegegevens en gegevens die betrekking hebben op de persoonlijke levenssfeer, worden gerekend.[65]

Een algemene geheimhoudingsbepaling voor ambtenaren is opgenomen in artikel 125a, derde lid, van de Ambtenarenwet. Daarin is bepaald dat de ambtenaar verplicht is tot geheimhouding van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt.

Een algemene geheimhoudingsplicht met betrekking tot persoonsgegevens is vastgelegd in artikel 9, vierde lid, Wbp. Daarin wordt bepaald dat de verwerking van persoonsgegevens achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat.

Naast deze algemene geheimhoudingsplichten bestaan ook tal van bijzondere geheimhoudingsbepalingen. Voor samenwerkingsverbanden op het terrein van de fraudebestrijding zijn vooral de geheimhoudingsbepalingen in de volgende wetten relevant: de Wjsg (art. 52), de Wpg (art. 7), de Algemene wet inzake rijksbelastingen (Awr, art. 67), de Wet op het financieel toezicht (Wft, art. 1:89 e.v.), de Wet controle op rechtspersonen (Wcr, art. 5, derde lid), de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Wet Bibob, art. 28) en de Wet Suwi (art. 74). Deze wetten bevatten ook bepalingen die het mogelijk maken de

---

[63] A.M. Klingenberg, A. Logemann en S.A.J. Munneke “Geheimhouding als juridische kwaliteitseis van primaire besluitvorming“ in: M. Herweijer, A.T. Marseille, F.M. Noordam, H.B. Winter (red), Alles in één keer goed. Juridische kwaliteit van bestuurlijke besluitvorming, 2005, blz. 178-179.

[64] De Moor-van Vugt, a.w. blz. 31.

[65] Kamerstukken II 1988-1989, 21221, nr. 3 blz. 57.

geheimhoudingsplicht te doorbreken, maar daaraan zijn dan vaak wel de nodige voorwaarden verbonden.

Zo kent de Wjsg in de artikelen 8a en 39f het College van procureurs-generaal de mogelijkheid toe om, voor zover dat nodig is met het oog op een zwaarwegend algemeen belang, justitiële, respectievelijk strafvorderlijke gegevens aan derden te verstrekken ten behoeve van specifiek omschreven doeleinden. Artikel 8a ziet daarbij op de justitiële documentatie waarover het OM de beschikking heeft gekregen in het kader van de behandeling van een strafzaak.[66] Het biedt dus geen grondslag om het OM justitiële gegevens te vragen waarover het OM zelf niet beschikt. Daarvoor zal, zo nodig, op grond van artikel 9 Wjsg een voorziening kunnen worden getroffen in het Besluit justitiële en strafvorderlijke gegevens (Bjsg). Voor zover het OM wel over justitiële en strafvorderlijke gegevens beschikt, heeft het OM in zijn beleidsregels bepaald dat, als aan bepaalde voorwaarden is voldaan, verstrekking ten behoeve van samenwerkingsverbanden mogelijk is.[67]

Ook de Wpg biedt de mogelijkheid om politiegegevens aan derden te verstrekken. Op grond van artikel 18 Wpg kan in het Besluit politiegegevens (Bpg) worden vastgelegd aan welke instellingen voor welke doeleinden politiegegevens kunnen worden verstrekt. Artikel 18 kent daarnaast aan de Minister van Veiligheid en Justitie de bevoegdheid toe in bijzondere gevallen toestemming of opdracht te geven tot het verstrekken van daarbij door hem te omschrijven politiegegevens, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang.[68] Verder biedt artikel 20 Wpg de korpschef de mogelijkheid in overeenstemming met het bevoegd gezag bepaalde politiegegevens aan samenwerkingsverbanden te verstrekken, voor zover dat noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor bepaalde doeleinden, zoals het voorkomen en opsporen van strafbare feiten.

Een algemene mogelijkheid om de geheimhoudingsplicht van artikel 67 Awr te doorbreken ten behoeve van de gegevensuitwisseling in samenwerkingsverbanden, ligt opgesloten in artikel 43c, eerste lid, onder m, van de Uitvoeringsregeling Awr. Ingevolge die bepaling kunnen gegevens worden verstrekt aan bepaalde bestuursorganen, voor zover deze gegevens nodig zijn om de samenwerking in het kader van de integrale toepassing en handhaving van overheidsregelingen effectief en efficiënt te laten verlopen en een convenant is gesloten met deze bestuursorganen.

De geheimhoudingsplicht die op grond van de Wft voor DNB en de AFM geldt, kan op grond van artikel 1:93 van die wet worden doorbroken ten behoeve van onder meer de Belastingdienst, de FIOD, de politie, het Bureau Financieel toezicht, de Financiële Inlichtingen Eenheid en het OM, voor zover de gegevens of inlichtingen dienstig zijn voor de uitoefening van hun wettelijke taken. Dat zou in beginsel ook kunnen gelden voor samenwerkingsverbanden waaraan één of meer van deze partijen deelnemen.

Op grond van artikel 5, derde lid, Wcr kan de daarin vastgelegde geheimhoudingsplicht worden doorbroken door bij AMvB toe te staan dat een organisatie die krachtens die wet de beschikking krijgt over gegevens met betrekking tot een derde die zijn neergelegd in een melding van een verhoogd risico van misbruik van een rechtspersoon, mededeling van dergelijke gegevens aan een andere organisatie doet. Op basis daarvan bepaalt artikel 5b van het Besluit controle rechtspersonen (Bcr) dat mededeling van dergelijke gegevens in een aantal daarin genoemde gevallen is toegestaan. Het gaat onder meer om verstrekking door de politie aan het openbaar

[66] Aanwijzing wet justitiële en strafvorderlijke gegevens, blz. 15-16.
[67] Het hangt van het samenwerkingsverband af of aan het samenwerkingsverband of (tegelijkertijd) aan de afzonderlijke deelnemers wordt verstrekt. Het samenwerkingsverband wordt dan aangemerkt als overige ontvanger als bedoeld in de Aanwijzing wet justitiële en strafvorderlijke gegevens .
[68] Van deze mogelijkheid is gebruik gemaakt om politiegegevens te verstrekken aan de RIEC's ten behoeve van de zgn. integrale casusanalyse. Zie Wpg-machtigingsbesluit RIEC's/werkproces integrale casusanalyse (Stcrt. 2013, nr. 6711).

ministerie, de RIEC's, de Koninklijke marechaussee, de Belastingdienst, de bijzondere opsporingsdiensten en de AIVD.

Ingevolge artikel 28, tweede lid, Wet Bibob mag het bestuursorgaan dat of de rechtspersoon met een overheidstaak die een Bibob-advies ontvangt, de daarin opgenomen gegevens doorgeven aan een aantal in die bepaling genoemde personen en organisaties. Daartoe behoren onder meer een andere deelnemer aan een RIEC, voorzover de gegevens noodzakelijk zijn voor het ondersteunen van het bestuursorgaan of de rechtspersoon met een overheidstaak bij het toepassen van de Wet Bibob.

De Wet Suwi kent naast de verschillende mogelijkheden tot bilaterale verstrekking in het Besluit Suwi, in artikel 64 de mogelijkheid gegevens te verstrekken aan samenwerkingsverbanden op een aantal terreinen van fraudebestrijding. Zodra partijen tot deelname aan een samenwerkingsverband hebben besloten, zijn zij ingevolge het derde lid van artikel 64 verplicht de noodzakelijke gegevens aan de andere partijen van het samenwerkingsverband te verstrekken.

Wat al deze mogelijkheden gemeen hebben, is dat zij weliswaar voor gegevensverstrekking aan samenwerkingsverbanden in verschillende mate enige ruimte geven, maar in de praktijk toch nog wel de nodige drempels opleveren. Zo geeft artikel 8a Wjsg toegang tot maar een deel van de justitiële gegevens. Verder lijkt de toetsing aan het criterium "zwaarwegend algemeen belang" bij de politie tot een zekere schroom te leiden om de mogelijkheden van artikel 20 Wpg te benutten. Het alternatief is gebruik maken van de mogelijkheid die artikel 9 Wjsg en 18 Wpg bieden om de verstrekking van gegevens aan samenwerkingsverbanden te regelen in het Bjsg, respectievelijk Bpg. De aard van die mogelijkheden brengt evenwel mee dat dit een regeling vergt voor ieder afzonderlijk samenwerkingsverband. Artikel 43c, eerste lid, onder m, van de Uitvoeringsregeling Awr biedt op het eerste gezicht veel ruimte voor verstrekking van belastinggegevens aan bepaalde bestuursorganen, maar stuit in de praktijk op toenemende terughoudendheid om deze ruimte te benutten, met name in gevallen waarin de doelstelling van een samenwerkingsverband wel erg algemeen is geformuleerd. Met de invoering van het huidige artikel 67 Awr in 2008 is als lijn neergezet dat nieuwe gevallen die in de uitvoeringsregeling worden opgenomen zoveel mogelijk worden beperkt en dat ernaar wordt gestreefd om gegevensverstrekking zoveel mogelijk bij wettelijk voorschrift te gaan regelen.[69] Ingeval van samenwerkingsverbanden zou dat evenwel kunnen impliceren dat voor ieder verband apart een wettelijke voorziening moet worden getroffen. Er lijkt inmiddels wel ruimte te bestaan voor verstrekking van gegevens door de Belastingdienst aan het OM, zonder dat daarvoor een vordering van het OM op grond van artikel 126nd Wetboek van Strafvordering (WSv) nodig is.[70] Die ruimte is echter nog niet bevestigd door de Hoge Raad.[71] De mogelijkheden om op grond van de Wft gegevens aan andere partijen te verstrekken, is vanwege het ingrijpende karakter van de informatieverplichtingen van financiële ondernemingen aan de toezichthouders aan strenge voorwaarden verboden.[72] De Wet Suwi biedt een goede basis voor gegevensuitwisseling, maar doet dat niet voor alle vormen van fraudebestrijding, laat staan voor andere doeleinden op het terrein van rechtshandhaving en criminaliteitsbestrijding. Tot slot valt erop te wijzen dat, voor zover een bepaalde wet al verstrekking van gegevens aan derden mogelijk maakt, deze mogelijkheden zich veelal beperken tot andere partijen binnen de overheid. De ruimte voor verstrekking aan private partijen is beperkt.

---

[69] De Moor-van Vugt, a.w., blz. 33.

[70] Zie Hof Arnhem-Leeuwarden 8-11-2013, ECLI:NL:GHARL:2013:8478. In dit arrest heeft het Hof uitgemaakt dat verstrekking van gegevens door de belastingdienst aan het OM zonder vordering mogelijk is, voor zover dit zijn basis vindt in een convenant tussen betrokken partijen. Tenzij het convenant dat zou uitsluiten, is verstrekking ook mogelijk in het geval dat de persoon om wiens gegevens het gaat, als verdachte wordt aangemerkt. Daaraan doet volgens het Hof niet af dat in dit geval ook toepassing had kunnen worden gegeven aan de regeling van artikel 126nd WSv. Zie in dit verband ook § 3.6.

[71] Een cassatieberoep dat tegen de in de vorige voetnoot genoemde uitspraak van het Hof Arnhem-Leeuwarden was ingesteld, is inmiddels ingetrokken.

[72] De Moor-van Vugt, a.w. blz. 33-34.

Wat zich hier wreekt, is dat, zoals ook hiervoor al is gesignaleerd, de verschillende mogelijkheden tot verstrekking van gegevens aan andere partijen hoofdzakelijk zijn geformuleerd vanuit het perspectief van de verschillende sectoren en niet met het oog op een overkoepelend publiek belang van samenwerkingsverbanden. De geheimhoudingsbepalingen in die sectorwetten gaan voor verstrekking aan dergelijke verbanden uit van "nee, tenzij". Een kaderwet zou dit paradigma kunnen doen kantelen naar "ja, tenzij". Het "nee, tenzij" leidt in de praktijk ertoe dat de discussie vooral gaat over wat mag en wat niet mag en daarmee primair een juridische discussie is. De kanteling naar "ja, tenzij" zal meebrengen dat de discussie een meer beleidsmatig karakter krijgt. Zij zal zich toespitsen op de vraag "Willen wij met elkaar samenwerken en de daartoe noodzakelijke gegevens uitwisselen en welke gegevens menen wij eventueel daarvan te moeten uitzonderen?".

Een en ander heeft niet tot doel de betekenis van geheimhoudingsbepalingen als zodanig ter discussie te stellen. Integendeel, geheimhoudingsbepalingen dienen, zoals aan het begin van deze paragraaf naar voren is gebracht, zeer legitieme belangen. Dit impliceert ook dat naar de mate waarin deze belangen meer gewicht hebben, de prudentie des te groter dient te zijn bij het benutten van de ruimte die een eventuele kaderwet zou bieden om in het specifieke geval van een samenwerkingsverband gegevens te verstrekken die in andere gevallen onder de werking van een geheimhoudingsplicht (blijven) vallen. Deze belangen kunnen zelfs een zodanig gewicht hebben dat een kaderwet de werking van geheimhoudingsbepalingen met betrekking tot bepaalde categorieën van gegevens onverkort in stand zou moeten laten. Dat geldt in het bijzonder ten aanzien van bepaalde categorieën van bijzondere persoonsgegevens (zie hiervóór § 2.4). Hoe dit in een kaderwet zou kunnen worden uitgewerkt, komt in § 4.4 aan de orde.

3.6 Gegevensverkrijging door opsporingsdiensten en OM

Voor het bestuursrechtelijke en het strafrechtelijke domein gelden verschillende wettelijke regimes. Dit houdt verband met het feit dat ten aanzien van personen die verdacht worden van een strafbaar feit, al naar gelang de aard en ernst van het feit, verdergaande bevoegdheden kunnen worden ingezet en aan deze personen zwaardere sancties kunnen worden opgelegd dan in het bestuursrecht mogelijk is. Daar staat tegenover dat voor verdachten op grond van internationale verdragen ook meer waarborgen gelden.

Het verschil in wettelijke regimes voor beide domeinen neemt niet weg dat bestuursrechtelijke handhaving, controle en toezicht in de praktijk kunnen overgaan in opsporing en vervolging zonder dat deze overgang altijd duidelijk is te markeren. Daar komt bij dat binnen het strafrechtelijk domein opsporingsdiensten en OM steeds vaker al activiteiten ontplooien vóór het moment waarop sprake is van een (vermoeden van een) strafbaar feit en van een mogelijke verdachte. Ook die ontwikkeling draagt eraan bij dat bestuursrechtelijke en strafrechtelijke handhaving naast elkaar kunnen gaan lopen. Dit gaat gepaard met een groeiende behoefte bij opsporingsdiensten en OM aan gegevens die andere organisaties hebben ten behoeve van het signaleren van trends en het maken van analyses om de criminaliteit beter te kunnen bestrijden. Het kan daarbij gaan om analyses in een concrete casus, waarbij partijen gezamenlijk bepalen welke interventies de meeste geschikte zijn om in de desbetreffende casus op te treden. Het kan ook gaan om een situatie die een meer pro-actief of preventief karakter heeft. Te denken valt aan het uitwisselen van gegevens om tot gezamenlijke "intelligence" te komen. Juist zulke vormen van samenwerking tussen bestuursrechtelijke toezichthouders en strafrechtelijke opsporingsinstanties kunnen bij uitstek meerwaarde hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtshandhaving en criminaliteitsbestrijding.

Deze ontwikkelingen mogen intussen niet de ogen doen sluiten voor een aantal wezenlijke factoren die bij verstrekking van gegevens vanuit het bestuursrechtelijk naar het strafrechtelijk domein een grote mate van prudentie vergen. Zo kent het WSv in de artikelen 126nc e.v. een uitgebalanceerd en uitgewerkt systeem voor het vorderen van informatie door opsporingsdiensten en OM in het

geval dat sprake is van een verdenking.[73] Dit hangt samen met de bevoegdheden die de opsporingsdiensten en het OM hebben om met die gegevens wat te doen. Wanneer het OM in het kader van een samenwerkingsverband over gegevens komt te beschikken die het vervolgens kan inzetten ten behoeve van opsporing en vervolging ontstaat een mogelijkheid voor het OM gegevens te verkrijgen buiten het WSv om, zonder de waarborgen die het WSv biedt.[74] Een tweede factor is dat artikel 6 EVRM de verdachte vanaf het moment waarop sprake is van een "criminal charge" rechten geeft waaronder bij voorbeeld het recht dat een verdachte niet zijn eigen veroordeling hoeft mee te werken (beginsel van "nemo tenetur"). Als onderdeel van het recht op een "fair trial" wordt gezien de noodzaak van het hebben van een "paper trail": er moet worden vastgelegd welke informatie waarvandaan komt. Aan de hand van de "trail" kan worden beoordeeld of de informatie rechtmatig is verkregen. Rechtmatige informatieverkrijging via samenwerkingsverbanden dient derhalve nauwkeurig te worden omschreven. Voorts verdient aandacht dat het bestuursrecht een ander bewijsrecht kent dan het strafrechtelijke systeem. In het bestuursrecht geldt de vrije bewijsleer. Conclusies kunnen worden getrokken en feiten kunnen komen vast te staan op basis van voldoende aannemelijkheid. Indien een feit dat aldus is komen vast te staan, wordt uitgewisseld met de opsporingsfase, kan dit ongemerkt op gespannen voet komen te staan met de strikte bewijsleer in het strafrecht. Tot slot wordt hier gewezen op het feit dat onder dwang verkregen informatie in de controlefase niet mag worden gebruikt als bewijs bij de boete (of de vervolging) in verband met het verbod op zelfincriminatie.[75]

Al deze factoren geven de burger een bepaalde mate van bescherming. Bij de verstrekking van gegevens vanuit het bestuursrechtelijk aan het strafrechtelijk domein binnen samenwerkingsverbanden zal daarom ook in de toekomt met deze factoren rekening moeten worden gehouden. Voor één van de genoemde factoren ware een uitzondering te maken. Dit betreft de verstrekking van identificerende en andere dan identificerende gegevens die niet gevoelig zijn, aan de politie en andere opsporingsdiensten, respectievelijk aan het OM waarvoor nu ingevolge artikel 126nc, respectievelijk 126nd WSv een vordering nodig is. De ratio voor een dergelijke vordering is dat de derde bij wie de gegevens worden gevorderd, in het algemeen minder goed in staat is tot het maken van een afweging over de verstrekking, omdat hij geen kennis draagt van alle achtergronden van het verzoek. Daarnaast is de derde in geval van vrijwillige medewerking verantwoordelijk en aansprakelijk voor de verstrekking van de gegevens.[76] Bestuursorganen die aan samenwerkingsverbanden deelnemen, zijn evenwel in het algemeen veel beter dan willekeurige anderen in staat tot het maken van een afweging over de verstrekking, omdat zij veelal wel enige kennis dragen van de achtergronden van het verzoek. Het is bij verstrekking door bestuursorganen dan ook niet altijd nodig de verantwoordelijkheid voor het vergaren van gegevens uitsluitend neer te leggen bij de met opsporing belaste instanties.

Nu de ratio achter de artikelen 126nc en 126nd WSv in het geval van gegevensuitwisseling binnen samenwerkingsverbanden vaak ontbreekt, levert het vereiste van een vordering een onnodige belemmering voor een efficiënte gegevensuitwisseling binnen samenwerkingsverbanden op.[77]

---

[73] Wanneer er géén sprake is van een verdenking, en dat zal in geval van gegevensuitwisseling in samenwerkingsverbanden vaak voorkomen, vindt de gegevensverwerking door opsporingsinstanties en OM plaats op grond van de algemene taakstellende artikelen van de Politiewet (artikel 3), de Wet op de bijzondere opsporingsdiensten (artikel 3) en het Wetboek van Strafvordering (artikelen 141 en 142). Dan mag er echter alleen een lichte inbreuk op de bescherming van de persoonlijke levenssfeer worden gemaakt. Zie o.a. HR 19 december 1995, NJ 1996, 249 (Zwolsman).

[74] Er is dan door de (lagere) wetgever bij het opnemen van een specifieke verstrekkingsbepaling kennelijk wel een expliciete overweging gemaakt dat een actieve verstrekking aan opsporingsinstanties en OM gerechtvaardigd is.

[75] EHRM 25-2-1993, NJ 1993, 485 (Funke), EHRM 17 -12-1996, NJ 1997, 699 (Saunders) en EHRM 3-5-2001, BNB 2002/26 (J.B. vs Zwitserland).

[76] Kamerstukken II, 2003-2004, 29 441, nr. 3, blz. 2.

[77] Tegen deze achtergrond heeft de Voorzitter van het College van Procureurs-Generaal de Minister van Veiligheid en Justitie bij brief van 4 juni 2012 verzocht de wetgeving op dit punt zo aan te passen dat een

Weliswaar lijkt er op grond van een arrest van het Hof Arnhem-Leeuwarden inmiddels ruimte te zijn voor verstrekking van gegevens door de Belastingdienst aan het OM zonder dat daarvoor een vordering van het OM op grond van artikel 126nd WSv nodig is[78], maar de Hoge Raad heeft het bestaan van deze ruimte nog niet bevestigd. Los van dit specifieke geval blijkt uit de jurisprudentie met betrekking tot artikel 126nd WSv dat een vordering door het OM als daarin bedoeld alleen dan achterwege kan blijven, indien de verstrekking van de desbetreffende gegevens niet alleen vrijwillig, maar ook uit eigen beweging geschiedt.[79] Aangenomen mag worden dat eenzelfde lijn geldt voor een vordering van identificerende gegevens als bedoeld in artikel 126nc. Zo lang deze lijn voor andere gevallen dan gegevensverstrekking door de Belastingdienst aan het OM blijft gelden en ook de ruimte voor gegevensverstrekking door de Belastingdienst nog ongewis is, blijft er sprake van een barrière voor de gegevensverstrekking aan de politie, andere opsporingsdiensten en het OM. Een eventuele kaderwet zou zo kunnen worden ingericht dat deze barrière verdwijnt. Daarbij zou rekening moeten worden gehouden met eventuele wensen van deelnemers aan een samenwerkingsverband omtrent het gebruik dat opsporingsdiensten en OM vervolgens van de ontvangen gegevens maken. Hoe daaraan invulling zou kunnen worden gegeven, komt in § 4.4 aan de orde.

3.7 Verstrekking van strafrechtelijke gegevens

In § 2.4 is naar voren gekomen dat de verwerking van bijzondere persoonsgegevens in beginsel verboden is (art. 16 Wbp). Wel bevat de Wbp een aantal uitzonderingen op dat verbod. Zo is het verbod om strafrechtelijke persoonsgegevens te verwerken, niet van toepassing, indien de verantwoordelijke deze heeft verkregen krachtens de Wpg of de Wjsg (art. 22, eerste lid, Wbp).

In de praktijk bestaat grote behoefte bij partijen die aan samenwerkingsverbanden deelnemen, aan betere mogelijkheden om strafrechtelijke gegevens door politie, bijzondere opsporingsdiensten en OM aan andere partijen binnen het samenwerkingsverband te laten verstrekken. Uit § 3.5 komt het beeld naar voren dat de mogelijkheden die de Wpg en de Wjsg bieden om strafrechtelijke persoonsgegevens aan samenwerkingsverbanden te verstrekken, echter niet optimaal zijn. Ook een recente wijziging van de Wet Suwi heeft daarin voor samenwerkingsverbanden op het terrein van de fraudebestrijding geen verandering gebracht.[80]

De mogelijkheden om strafrechtelijke persoonsgegevens te verstrekken, kunnen worden verbeterd door in de Wpg en Wjsg bepalingen op te nemen die een algemene grondslag voor gegevensverstrekking aan samenwerkingsverbanden als bedoeld in de kaderwet geeft. Een dergelijke algemene grondslag zou impliceren dat het niet meer nodig zou zijn om voor ieder samenwerkingsverband afzonderlijk een basis voor gegevensuitwisseling in het Bpg, respectievelijk het Bjsg te leggen.

3.8 Typen van verwerking

De behoefte aan gegevensuitwisseling bestond in het verleden vooral uit informatie in een concreet geval. Deze behoefte bestaat nog steeds, maar wordt langzamerhand overvleugeld door de behoefte aan gegevens ten behoeve van grootschalige bestandsvergelijkingen voor het onderkennen van trends en patronen en het opstellen van profielen. De ontwikkeling van geavanceerde analysetechnieken onder de noemer van "big-data-analytics" is daar mede debet aan. Met het oog op deze ontwikkeling wordt in de kabinetsbrief van 20 december 2013 over de aanpak van fraude ervan uitgegaan dat de verkenning mede betrekking heeft op de mogelijkheden om op verkennende wijze fraudepatronen te onderkennen.[81]

---

gegevensverstrekking binnen een samenwerkingsverband mogelijk is zonder dat daaraan een vordering op grond van het stelsel van strafvorderlijke bevoegdheden ten grondslag ligt.

[78] Zie Hof Arnhem-Leeuwarden 8-11-2013, ECLI:NL:GHARL:2013:8478. Zie ook § 3.5.

[79] HR 27-11-2012, LJN BY0215.

[80] Zie kamerstukken II 2012-2013, 33579, nr. 3, blz. 22.

[81] Kamerstukken II 2013-2014, 17050, nr. 450, blz. 7.

De praktijk worstelt met de vraag of en, zo ja, in hoeverre de huidige regelgeving allerlei typen van gegevensverwerking binnen samenwerkingsverbanden toestaat. Dat geldt vooral voor de eerder bedoelde moderne analysemethoden. Mag bijvoorbeeld iCOV aan de hand van een gerichte selectie van naar verwachting relevante databestanden met behulp van geavanceerde software mogelijk relevante patronen in beeld brengen die dit samenwerkingsverband kan gebruiken voor het opstellen van profielen? En mag iCOV een door haar te ontwikkelen profiel van bijvoorbeeld beroepsfraudeurs matchen met alle data waarover zij rechtmatig de beschikking heeft, om een lijst vast te stellen van personen aan wie de grootste risico's zijn verbonden dat zij fraude plegen?

De thans bestaande onduidelijkheid op dit punt belemmert de ontwikkeling en het gebruik van diensten en producten die met moderne analysemethoden geleverd kunnen worden. Dit vloeit niet alleen voort uit het veelal ontbreken van bepalingen in de huidige regelgeving die specifiek betrekking hebben op samenwerkingsverbanden[82], maar ook uit het ontbreken van bepalingen over de wijze van gegevensverwerking. Er zijn slechts enkele wettelijke bepalingen die iets zeggen over geautomatiseerde gegevensverstrekking of het geautomatiseerd zoeken in de eigen systemen op verzoek van een derde waarna de gegevens separaat (door tussenkomst van een medewerker) worden verstrekt.[83]

Een kaderwet gegevensuitwisseling zou de bestaande onduidelijkheid kunnen wegnemen door uitdrukkelijk te bepalen dat de door deze wet gereguleerde gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in die wet beschreven typen van verwerking. Deze typen zouden in beginsel alle typen gegevensuitwisseling moeten beslaan die in § 2.5 zijn beschreven. In § 4.6 wordt dit nader uitgewerkt.

3.9 Kwaliteit gegevens en zorgvuldigheid bij verwerking

De Wetenschappelijke Raad voor het Regeringsbeleid heeft in zijn rapport iOverheid uit 2011 aangegeven dat voor het bewaken van de kwaliteit van gegevens rekening dient te worden gehouden met een drietal ontwikkelingen:

1. het vernetwerken van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren,
2. het samenstellen en verrijken van informatie, d.w.z. het creëren van nieuwe informatie en profielen op basis van verschillende bronnen uit verschillende contexten,
3. het voeren van preventief en proactief beleid op basis van informatie, d.w.z. het actief beoordelen van en ingrijpen in de samenleving op basis van informatiegestuurde risicoprofielen.

Deze ontwikkelingen brengen mee dat gegevens die uit bronnen met verschillende, soms zeer uiteenlopende doeleinden worden geput, eerst worden gedecontextualiseerd om vervolgens te worden gehercontextualiseerd, wanneer zij worden gecombineerd met andere gegevens in een andere beleidscontext. Daaraan kleven risico's voor de kwaliteit van de gegevens in termen van betrouwbaarheid en kenbaarheid. Dat geldt voor de professionals die met deze gegevens moeten werken (en informatie uit een andere professionele context moeten interpreteren) en wordt nog versterkt wanneer het gaat om informatie die het resultaat is van technische bewerkingen, zoals "profiling" en "datamining". Aandacht voor de kwaliteit van informatie vereist ook gedegen aandacht voor technische en organisatorische randvoorwaarden zoals beveiliging, werkprocessen en een betrouwbare authenticatie- en identificatie-infrastructuur.[84]

De hier geschetste ontwikkelingen doen zich vooral ook voor bij gegevensuitwisseling in samenwerkingsverbanden. Bij een onderzoek naar gegevensuitwisseling door toezichthouders

[82] Uitzonderingen zijn te vinden in artikel 22, zesde lid, Wbp, artikel 20 Wpg, artikel 28, tweede lid, onder d, Wet Bibob en artikel 64 Wet Suwi. Zie ook § 3.2.
[83] Voorbeelden hiervan zijn artikel 23 Wpg, artikel 107c Kadasterwet en artikel 28 Handelsregisterwet 2007.
[84] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid, 2011, blz. 214-217.

brachten experts naar voren dat onder andere politiegegevens niet altijd even hard zijn. Welke hardheidsgraad de gegevens hebben, is vaak niet bekend. De gegevens kunnen uit meerdere bronnen komen, of het relaas kan onvolledig zijn. Dat is niet goed te controleren. Databestanden kunnen daardoor "vervuild" zijn met zachte informatie. Verder blijkt uit het onderzoek het risico dat gegevens niet helemaal betrouwbaar zijn wanneer deze binnen een gegevensverzameling worden verrijkt met subjectieve informatie. Dit leidt tot kleuring van de gegevens, die in een andere context en binnen een andere gegevensverzameling verkeerd of onjuist kan worden opgevat. Omgekeerd kunnen gegevens worden gefilterd alvorens zij worden verstrekt aan een andere partij, waardoor belangrijke elementen verloren kunnen gaan.[85]

Wil een kaderwet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverbanden opleveren, dan zal deze kaderwet niet alleen een verruiming van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voorzieningen moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan. In § 4.7 zal worden ingegaan op de vraag welke voorzieningen dat zouden kunnen zijn.

3.10 Verantwoordelijke

Het is uit een oogpunt van privacybescherming van belang duidelijk vast te stellen wie met betrekking tot de gegevensverwerking als verantwoordelijke in de zin van de Wbp is aan te merken. Op deze verantwoordelijke rusten immers verschillende verplichtingen, zoals de informatieplicht, de beveiligingsplicht, de meldingsplicht en de verplichting betrokkenen gebruik te kunnen laten maken van hun inzage–en correctierecht.

Als er sprake is van een samenwerkingsverband, roept dat discussie op over de vraag wie verantwoordelijke is voor de gegevensverwerking binnen het samenwerkingsverband. In een kaderwet zou, in navolging van artikel 64, tweede lid, van de Wet Suwi, als uitgangspunt kunnen worden gekozen voor een gezamenlijke verantwoordelijkheid van de deelnemers aan het samenwerkingsverband. Dit uitgangspunt komt overeen met de keuze die men, gelet op het geïntegreerde karakter van de verschillende verwerkingen, nu meestal in de praktijk maakt. Het is evenwel denkbaar dat de verschillende verwerkingen een andere keuze rechtvaardigen. Er kan bijvoorbeeld sprake zijn van afzonderlijke verantwoordelijkheid per (deel)verwerking. Ook kan de situatie bestaan dat, ook al nemen aan de verwerkingen verschillende organisaties deel, er voor één gemeenschappelijke verantwoordelijke wordt gekozen.[86] Met het oog op deze mogelijkheden zal een kaderwet ruimte dienen te bevatten om van het in die wet gekozen uitgangspunt af te wijken.

3.11 Informatieplicht

In de praktijk blijkt dat samenwerkingsverbanden vaak worstelen met de vraag of en, zo ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 34 Wbp. Die vraag speelt vooral in het geval van grootschalige geautomatiseerde bestandsvergelijkingen in een fase die voor het overgrote deel van de betrokkenen niet tot gevolgen leidt. De informatieplicht houdt in dat de betrokkenen door de verantwoordelijke worden geïnformeerd over de verwerking van hun persoonsgegevens. Deze plicht is niet van toepassing, indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot vastlegging of verstrekking van de hem betreffende gegevens heeft geleid (art. 34, vijfde lid, Wbp).

De keuze voor een kaderwet zou het mogelijk maken van deze uitzondering op de informatieplicht gebruik te maken. Daarvoor zou dan wel nodig zijn dat uit die kaderwet blijkt dat, indien partijen een samenwerkingsverband oprichten, zij – uitzonderingen daargelaten – verplicht zijn de

---

[85] De Moor-van Vugt, a.w., blz. 51-57 en 75.
[86] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 58.

noodzakelijke gegevens aan dat samenwerkingsverband te verstrekken.[87] Het zou de transparantie voor de burger bevorderen, als in de kaderwet ook zou worden bepaald dat bij de oprichting van een samenwerkingsverband ervoor wordt gezorgd dat er algemene informatie wordt gegeven over de gegevensverwerking door het desbetreffende samenwerkingsverband. Deze informatie zou dan bijvoorbeeld op een website kunnen worden geplaatst. Met het oog daarop zou de kaderwet de verplichting kunnen bevatten in het informatieprotocol bepalingen op te nemen met betrekking tot de informatieverstrekking over de gegevensuitwisseling aan het publiek (zie nader § 4.10).

Een dergelijke regeling in een kaderwet zou dus meebrengen dat niet iedere betrokkene afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar. Dat heeft het voordeel dat alle inspanningen die hiervoor nodig zijn, achterwege kunnen blijven, zonder dat het noodzakelijk is precies na te gaan of die inspanningen zijn aan te merken als een onevenredige inspanning, die ingevolge het vierde lid van artikel 34 eveneens kan leiden tot het buiten toepassing laten van de informatieplicht. Belangrijker is dat het in samenwerkingsverbanden op het terrein van de fraudebestrijding al gauw gaat om gegevensverwerking die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden.[88]

3.12 Vertrouwen in het gebruik van gegevens door andere partijen

Bij gegevensuitwisseling in samenwerkingsverbanden geldt dat geen enkele partij graag gegevens verstrekt, als niet duidelijk is wat ermee gebeurt. Dat geldt vooral als het om gevoelige gegevens gaat. Het bestaan van onduidelijkheid op dit punt kan een belemmering vormen voor de gegevensuitwisseling. Het gaat hier vooral om de vraag of verstrekking aan derden buiten het samenwerkingsverband mogelijk moet zijn en, zo ja, onder welke voorwaarden. Als hierover onduidelijkheid bestaat, wordt mogelijk in strijd gehandeld met het zorgvuldigheidsbeginsel, dat in artikel 6 Wbp is verankerd.[89]

Om voldoende vertrouwen in het gebruik van gegevens door andere partijen te kunnen hebben, wordt soms het "gazo"-principe gehanteerd: geen actie zonder overleg. Dit gebeurt bijvoorbeeld bij samenwerkingsverbanden die te maken hebben met meldingen op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), zoals het FEC. Verder is denkbaar dat expliciet wordt vastgelegd dat doorverstrekking aan een derde alleen plaatsvindt met instemming van de partner van wie de persoonsgegevens oorspronkelijk afkomstig zijn.[90] Met het oog daarop kan het zinvol zijn doorverstrekking aan derden te "loggen". In een kaderwet kunnen op dit punt bepaalde voorzieningen worden getroffen.

---

[87] Vgl. artikel 64, tweede lid, Wet Suwi.
[88] Zie ook kamerstukken II 2012-2013, 33579, nr. 3, blz. 26.
[89] Vgl. ABRvS 4 juli 2007, overweging 2.4.5, LJN: BA8742, 200608203/1.
[90] Zie de artikelen 4 en 18 Informatieprotocol FEC 2011, Stcrt. 2011, 21708.

4. Contouren kaderwet

4.1 Inleiding

In de vorige paragraaf is aangegeven dat de daarin genoemde knelpunten kunnen worden weggenomen door een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden. In deze paragraaf worden de contouren van zo'n kaderwet geschetst. Daarvoor is mede gebruik gemaakt van elementen uit een recente wet tot wijziging van de Wet Suwi.[91] Deze wijzigingswet bevat een nieuw artikel 64 Wet Suwi, waarin een regeling voor de gegevensverstrekking ten behoeve van samenwerkingsverbanden is opgenomen. Aan het slot van deze paragraaf wordt achtereenvolgens ook ingegaan op de rechtsbescherming en het toezicht, de verhouding van de kaderwet tot de bestaande wetgeving, de betekenis van de kaderwet voor bestaande samenwerkingsverbanden en de verhouding van de kaderwet tot het EVRM en regelgeving van de EU.

Een belangrijk kenmerk van het nieuwe artikel 64 Wet Suwi is dat het niet geschreven is voor één specifiek samenwerkingsverband. Daarmee heeft dit artikel al enigszins het karakter van een kaderregeling. Een verschil met een kaderwet, zoals bedoeld in deze notitie, is dat de reikwijdte van artikel 64 beperkter is dan van zo'n kaderwet. Dat artikel bestrijkt maar een – overigens niet onbelangrijk - deel van de mogelijke vormen van fraude en bevat vanwege die relatief beperkte reikwijdte een aantal elementen, zoals de (gedeeltelijke) samenstelling van een samenwerkingsverband[92], die in een kaderwet uit een oogpunt van flexibiliteit geheel aan regeling bij convenant zouden moeten worden overgelaten. Een ander verschil is dat artikel 64 blijkens de toelichting uitsluit dat aan het samenwerkingsverband ook strafrechtelijke persoonsgegevens worden verstrekt.[93]

Een kaderwet (of raamwet) is een wet die de algemene principes, verantwoordelijkheden en procedures regelt, maar geen gedetailleerde regels bevat. Een belangrijke eigenschap van kaderwetten lijkt dan ook dat zij doorgaans niet zelf beleidsinhoudelijke regulatieve keuzes vastleggen, maar vooral randvoorwaarden scheppen waarbinnen bijvoorbeeld lagere regelgevers, beleidsmakers of uitvoerders dienen te opereren.[94] Een kaderwet zal in dat licht bezien niet voor ieder samenwerkingsverband in detail regelen waaraan dat samenwerkingsverband zich heeft te houden. Dat zou ook niet goed mogelijk zijn zonder te vervallen in een rigide structuur die onvoldoende ruimte voor maatwerk voor ieder afzonderlijk samenwerkingsverband biedt.[95] Wel zal een kaderwet een raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking nader uitwerken in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. Een kaderwet kan daarbij de knelpunten wegnemen die nu in de praktijk bij het opstellen van zo'n convenant en protocol worden ervaren. Een kaderwet zou echter niet alleen legitimerend en faciliterend, maar ook normerend moeten zijn.[96] Zij zou de hoofdlijnen moeten bevatten voor een aantal waarborgen voor een zorgvuldige gegevensuitwisseling, die in het convenant en het informatieprotocol van een samenwerkingsverband nader moeten worden uitgewerkt.

---

[91] Wet van 9 oktober 2013 tot wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekende zijnde gegevens, Stb. 2013, 405.

[92] Artikel 64, eerste lid, van de Wet Suwi noemt de colleges van burgemeester en wethouders, het UWV, de SVB, toezichthouders op het terrein van SZW, de Belastingdienst en andere bestuursorganen en personen, voor zover zij zijn belast met een publieke taak en daartoe bij regeling van de Ministers van SZW en Financiën zijn aangewezen.

[93] Kamerstukken II 2012-2013, 33579, nr. 3, blz. 22.

[94] R.A.J. van Gestel en A. Vleugel, Herijking van het primaat van de wetgever: de betekenis van de kaderwetgeving en delegatie, 2012, blz. 19.

[95] De werkgroep herijking toezichtregelgeving kwam in 2008 met betrekking tot de gegevensuitwisseling tussen toezichthouders tot dezelfde conclusie. Zie § 2.8.

[96] De Moor-van Vugt, a.w., blz. 59.

Gelet op het kabinetsstandpunt over het WODC-rapport "Gegevensuitwisseling door toezichthouders" zal een kaderwet ook niet het karakter kunnen krijgen van een wet waarin de huidige Wbp wordt omgevormd tot een brede kaderwet, eventueel met nadere uitwerking in sectorale wetgeving. Het kabinet heeft in reactie op dat rapport zich immers – zie § 2.7 - op het standpunt gesteld dat een meer algemene bezinning op het huidige nationale kader beter kan wachten op de uitkomst van de herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens. Dat impliceert dat het nu niet opportuun is voor een kaderwet te pleiten waarin de Wbp opgaat. Het kabinetsstandpunt laat wel ruimte voor een meer bescheiden opzet van een kaderwet, waarbij de Wbp, de Wpg, de Wjsg en de bepalingen over gegevensverwerking in sectorale wetten, op mogelijk een enkele kleine aanpassing na, in stand blijven. Deze opzet zou niet alleen het voordeel hebben dat de voorbereiding van een dergelijke kaderwet niet of nauwelijks zou interfereren met de lopende herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens en het vervolg op de evaluatie van de Wpg en Wjsg. Zij zou ook de voorkeur verdienen, omdat bij een keuze voor een brede kaderwet waarin de Wbp opgaat, voorbij zou worden gegaan aan het feit dat de Wbp ook betekenis heeft voor al die vormen van gegevensverwerking die buiten samenwerkingsverbanden plaatsvinden. Hetzelfde geldt met betrekking tot de Wpg en Wjsg en bepalingen over gegevensverwerking in sectorale wetten, voor zover de gedachte zou bestaan deze regelgeving of delen daarvan eveneens in zo'n brede kaderwet op te nemen. Een kaderwet met deze opzet zou aldus ook geen alles omvattend kader voor gegevensuitwisseling in samenwerkingsverbanden bieden. De Wbp, Wpg, Wjsg en de bepalingen over gegevensverwerking in sectorale wetten zullen ook in relatie tot samenwerkingsverbanden die onder de werking van de kaderwet vallen, hun betekenis blijven houden, tenzij een specifieke bepaling uit de kaderwet deze terzijde schuift (zie nader § 4.12). In zoverre dekt de term "kaderwet" niet geheel de lading. Aan de andere kant is de term "kaderwet" in die zin wel op haar plaats, nu zij ten opzichte van eerder bedoelde regelingen een aanvullend kader voor gegevensuitwisselingen in samenwerkingsverbanden geeft, waarbinnen een convenant en een informatieprotocol nadere regels over deze gegevensuitwisseling dienen te bevatten.

Tot slot valt erop te wijzen dat een kaderwet voor gegevensuitwisseling een algemene aanvulling zou vormen op wettelijke regelingen die in specifieke gevallen samenwerking voorschrijven en daarbij regels over gegevensuitwisseling geven, zoals de in artikel 9 van de Wet Suwi voorgeschreven samenwerking tussen het UWV, de SVB en de gemeenten bij de uitvoering van die wet en enige andere wetten. Deze aanvulling impliceert niet dat ook de kaderwet samenwerking tussen overheidsorganisaties voorschrijft. Dat zou, gelet op de vele, soms zeer uiteenlopende belangen van deze organisaties, niet kunnen. De aanvullende betekenis van een kaderwet zal wel zijn gelegen in het feit dat, àls partijen tot samenwerking besluiten en de uitwisseling van gegevens onder de werking van de kaderwet willen laten vallen, deze kaderwet de uitwisseling van gegevens in zo'n samenwerkingsverband legitimeert, faciliteert en normeert. Hiermee is ook gezegd dat de kaderwet niet tot doel heeft een exclusief regime voor gegevensuitwisseling in samenwerkingsverbanden te creëren. Het staat huidige en toekomstige samenwerkingsverbanden vrij ervoor te kiezen hun gegevensverwerking in te richten op grond van de thans al geldende wetgeving. Daartoe kan aanleiding bestaan, indien de kaderwet voor een samenwerkingsverband, gelet op haar behoeften aan informatie, niet of nauwelijks betere mogelijkheden tot gegevensuitwisseling boven de bestaande wetgeving biedt.

Tegen de achtergrond van deze overwegingen zou een kaderwet de elementen kunnen bevatten die in de volgende paragrafen worden beschreven.

4.2 Reikwijdte kaderwet

In de brief van het kabinet van 20 december 2013 over de aanpak van fraude wordt de verkenning naar een kaderwet toegespitst op fraudebestrijding. De aard van de kabinetsbrief brengt dat begrijpelijkerwijs mee. De vraag rijst evenwel of een kaderwet gegevensuitwisseling in samenwerkingsverbanden zich tot dat domein zou moeten beperken.

Zoals in § 2.3 al naar voren is gekomen, houdt van de samenwerkingsverbanden die zich met fraudebestrijding bezighouden, in feite een minderheid zich uitsluitend met fraudebestrijding bezig. De meeste samenwerkingsverbanden hebben een taak die zich in meerdere of mindere mate ook tot andere terreinen uitstrekt. Een kaderwet die zich beperkt tot gegevensuitwisseling ten behoeve van de fraudebestrijding zou tot gevolg hebben dat samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van de kaderwet vallen. Dat zou voor die samenwerkingsverbanden een onwerkbare situatie opleveren. Het zou al lastig zijn, als gegevens voor uitsluitend één doel zouden worden verwerkt. Gegevens die samenwerkingsverbanden verwerken, kunnen echter meerdere doelen tegelijk dienen. Zo kunnen de RIEC's bepaalde persoonsgegevens verwerken met het oog op tegelijkertijd georganiseerde hennepteelt èn fraude in de vastgoedsector. Het is dan niet doenlijk deze verwerking te laten plaatsvinden onder de gelijktijdige werking van de kaderwet en van daarvan afwijkende bepalingen in andere wetgeving.

Los van deze overweging kan worden vastgesteld dat een kaderwet voor veel meer samenwerkingsverbanden in de publieke sfeer betekenis kan hebben dan alleen de verbanden die (mede) op het terrein van de fraudebestrijding bezig zijn. Geluiden uit de praktijk bevestigen dit. Bij een relatief smalle kaderwet zou dus al gauw de behoefte ontstaan om voor aanpalende terreinen eveneens kaderwetgeving op te stellen. Dat pleit voor een kaderwet die een breder domein dan fraudebestrijding bestrijkt. Gekozen zou dan kunnen worden voor een kaderwet op het brede terrein van de voorkoming van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen, de uitoefening van toezicht op de naleving van wettelijke voorschriften en de handhaving van de openbare orde en veiligheid ("bestuursrechtelijke preventie en handhaving") en de voorkoming, opsporing en vervolging van strafbare feiten ("strafrechtelijke preventie en handhaving"). Het is immers dit brede terrein waarop zich allerlei samenwerkingsverbanden manifesteren die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen.[97]

Bezien vanuit de overheid kan de relatie van burgers en overheid worden getypeerd in drie categorieën: dienstverlening, zorg en controle. In dat licht bezien zou een kaderwet met de hiervóór voorgestelde reikwijdte zich richten op de controletaak van de overheid. Het gaat hier om een weliswaar breed, maar wel samenhangend terrein, waarop de overheid verschillende functies vervult. Deze variëren van toetsing van de antecedenten van een burger die een vergunning aanvraagt, tot de vervolging van een burger die een strafbaar feit pleegt. Dit neemt niet weg dat de drie genoemde categorieën in analytische zin weliswaar van elkaar te onderscheiden zijn, maar in praktische zin sterk door elkaar lopen.[98] Voor het uitvoeren van de controletaak wordt immers regelmatig een beroep gedaan op gegevens die oorspronkelijk op de andere terreinen – dienstverlening en zorg – zijn verkregen. Niettemin zal bij het uitwerken van een kaderwet – mede met het oog op het principe van doelbinding - rekening moeten worden gehouden met het feit dat het hier om verschillende terreinen gaat. Dat geldt met name voor gegevens op het terrein van de zorg, omdat het op dat terrein om bijzondere persoonsgegevens kan gaan. Te denken valt aan gegevens met betrekking tot iemands gezondheid, waarvoor het medisch beroepsgeheim geldt. Welke consequenties hieraan voor een eventuele kaderwet moeten worden verbonden, komt in § 4.4 aan de orde.

Erkend zij dat ook een kaderwet op een breed terrein als de controletaak van de overheid het probleem kan oproepen van de toepasbaarheid op samenwerkingsverbanden die op zowel het terrein van de kaderwet als daarbuiten opereren. Naarmate het terrein dat de kaderwet beslaat, groter is, zal dit probleem zich naar verwachting evenwel minder snel voordoen. Daarbij moet worden bedacht dat bijvoorbeeld de gegevensverwerking binnen veiligheidshuizen volledig onder de reikwijdte van zo'n bredere kaderwet is te vatten. Weliswaar nemen aan veiligheidshuizen ook partners uit de zorg deel, maar het doel van veiligheidshuizen en daarmee ook van de gegevensverwerking staat in het teken van het terugdringen van overlast, huiselijk geweld en

---

[97] Hoe een kaderwet met deze strekking zich tot de bestaande wetgeving zou verhouden, komt in § 4.12 aan de orde.

[98] De Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid, 2011, blz. 72.

criminaliteit en valt daarmee onder de noemer van handhaving van de openbare orde en veiligheid en voorkoming van strafbare feiten en aldus onder de reikwijdte van zo'n bredere kaderwet.[99]

Een andere vraag die de reikwijdte van een eventuele kaderwet bepaalt, is de vraag of deze wet alleen voor samenwerkingsverbanden zou moeten gelden die op nationaal niveau opereren, of ook voor verbanden die op regionaal of lokaal niveau werkzaam zijn. Met het oog op de belangen die de kaderwet wil dienen, ligt een beperking tot samenwerkingsverbanden op nationaal niveau niet voor de hand. Juist op lokaal en regionaal niveau bestaan samenwerkingsverbanden die maatwerk vergen, waarvoor een kaderwet een legitimerende, faciliterende en normerende functie kan uitoefenen.

Voor de reikwijdte van een kaderwet is tot slot van belang of aan samenwerkingsverbanden die onder de kaderwet vallen, ook private partijen mogen deelnemen. Om de redenen die in § 2.3 zijn genoemd, valt daar veel voor te zeggen. Omdat het delen van informatie tussen publieke en private partijen gevoelig ligt, is het wenselijk dat de kaderwet voldoende waarborgen bevat dat de gegevensuitwisseling een te rechtvaardigen doel dient. De belangrijkste waarborg is dat dit doel een publiek belang dient te zijn; verstrekking van gegevens aan private partijen met het oog op bijvoorbeeld commerciële belangen van die partijen is ongewenst. Met een kaderwet die betrekking heeft op gegevensuitwisseling met als doel de bestuursrechtelijke en strafrechtelijke preventie en handhaving te bevorderen, is dat publieke belang verzekerd. Een andere waarborg is dat de kaderwet de kring van private partijen die aan samenwerkingsverbanden kunnen deelnemen, beperkt tot partijen die een relatie tot enig publiek belang hebben. Dat belang kan zich uiten in het feit dat het om private partijen gaat die een wettelijke taak hebben. Het zou daarbij ook om koepel- of brancheorganisaties van dergelijke partijen kunnen gaan. Met deze beperking valt te denken aan banken, die op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme een zgn. cliëntenonderzoek moeten houden. Bij brancheorganisatie kan in dit verband worden gedacht aan het Verbond van verzekeraars, nu ook verzekeraars een dergelijk cliëntenonderzoek moeten houden. Omdat niet geheel op voorhand valt te overzien of er niet nog andere private partijen zijn die op goede gronden aan een samenwerkingsverband zouden kunnen deelnemen, lijkt het wenselijk te bepalen dat private partijen ook dan aan een samenwerkingsverband onder de reikwijdte van deze wet kunnen deelnemen, indien zij voorkomen op een lijst die bij ministeriële regeling is vastgesteld.[100] Daarmee dragen de ministers op wier beleidsterrein het desbetreffende samenwerkingsverband functioneert, ingeval van deelname van private partijen van deze lijst mede verantwoordelijkheid voor de samenstelling van het verband en kunnen zij daarop door het parlement worden aangesproken. Dit kan vooral van belang zijn bij regionale of lokale samenwerkingsverbanden waarvoor de ministeriële verantwoordelijkheid, afhankelijk van de deelnemers van overheidszijde, niet of slechts in beperkte mate aanwezig zou zijn.

Als resumé van voorgaande bespiegelingen bepleit de werkgroep een eventuele kaderwet zo in te richten dat zij betrekking heeft op samenwerkingsverbanden die voor een specifiek doel binnen het brede kader van bestuursrechtelijke en strafrechtelijke preventie en handhaving werkzaam zijn, op zowel nationaal, regionaal als lokaal niveau, en waaraan ook private partijen kunnen deelnemen.

4.3 Regeling samenwerkingsverband in convenant

Een kaderwet gegevensuitwisseling in samenwerkingsverbanden zou in de eerste plaats moeten bepalen dat bestuursorganen[101] en private partijen aan een samenwerkingsverband kunnen

---

[99] Zie voor het doel en de opzet van veiligheidshuizen: http://veiligheidshuizen.nl/achtergrond.
[100] Gedacht kan worden een lijst die is vastgesteld door de Minister van Veiligheid en Justitie en de Minister op wiens beleidsterrein de desbetreffende organisatie werkzaam is. Bij deelname van bijvoorbeeld het Verbond van verzekeraars gaat het dan om de Minister van Financiën.
[101] Het feit dat hier over bestuursorganen wordt gesproken sluit uiteraard niet uit dat in de praktijk een door een bestuursorgaan gemachtigde persoon, dienst of instelling aan het samenwerkingsverband deelneemt en met het oog daarop ook het convenant ondertekent.

deelnemen ten behoeve van een integraal optreden in het belang van de voorkoming van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen, de uitoefening van toezicht op de naleving van wettelijke voorschriften, de handhaving van de openbare orde en veiligheid en de voorkoming, opsporing en vervolging van strafbare feiten. Hiermee zou een kaderwet het bredere doel omschrijven waarbinnen samenwerkingsverbanden voor een meer specifiek doel kunnen worden aangegaan. Met integraal optreden wordt in dit verband bedoeld dat de deelnemers aan een samenwerkingsverband tot een integrale weging van alle relevante informatie komen, opdat zij daarop hun optreden kunnen baseren. Het hoeft niet te betekenen dat ook alle deelnemers tot actie overgaan. Dat hangt af van wat als het meest effectieve optreden wordt gezien.

De kaderwet zou vervolgens moeten bepalen dat de deelnemers aan het samenwerkingsverband in een convenant nauwkeurig het specifieke doel van de samenwerking en de daarvoor noodzakelijke gegevensuitwisseling vastleggen. Dit doel moet passen binnen de reikwijdte van de bredere wettelijke doelomschrijving en niet onverenigbaar zijn met het doel waarvoor de gegevens die aan het samenwerkingsverband worden verstrekt, oorspronkelijk zijn verzameld. Als het huidige voorstel voor een Algemene verordening gegevensbescherming wordt aangenomen, zal er ruimte ontstaan om bij onverenigbaarheid van doelen in een samenwerkingsverband toch tot gegevensuitwisseling over te gaan (zie § 3.4). Bij de voorbereiding van een eventuele kaderwet zal hiermee rekening moeten worden gehouden.

De brede wettelijke doelomschrijving kan uiteraard niet tot gevolg hebben dat samenwerkingsverbanden worden opgericht die over de volle breedte daarvan zullen gaan opereren. De verenigbaarheidstoets die artikel 9 Wbp voorschrijft, zou daar al gauw een stokje voor steken. De oprichting van dergelijke zeer brede samenwerkingsverbanden zou bovendien op gespannen voet staan met het in artikel 8 EVRM verankerde vereiste van noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit (zie hierna § 4.7). Deelnemers aan een samenwerkingsverband zullen het specifieke doel van het samenwerkingsverband en de daarvoor noodzakelijke gegevensuitwisseling dan ook steeds moeten kunnen verdedigen in het licht van dit vereiste en deze beginselen. Dat is nu al zo en zal onder de werking van de kaderwet niet veranderen.

Over de vraag of een samenwerkingsverband onder de werking van de kaderwet valt, mag geen misverstand bestaan. Dit geldt te meer, nu de kaderwet – zie § 4.1 – geen exclusief regime voor samenwerkingsverbanden beoogt te zijn. Om die reden zullen de deelnemers aan een samenwerkingsverband in hun convenant uitdrukkelijk moeten aangeven dat het samenwerkingsverband onder de werking van de kaderwet valt. Dat impliceert uiteraard dat zij niet alleen de beschikking over betere mogelijkheden tot gegevensuitwisseling krijgen, maar ook aan de extra waarborgen moeten voldoen die in § 4.7 aan de orde komen.

De kaderwet zou kunnen bepalen dat het convenant naast het specifieke doel van het samenwerkingsverband in ieder geval ook het volgende regelt:

a. de taken en werkzaamheden die binnen het samenwerkingsverband worden uitgevoerd,
b. de wijze waarop het samenwerkingsverband wordt bestuurd,
c. de inrichting van een eventueel bureau dat het samenwerkingsverband ondersteunt,
d. de rechten en de verplichtingen van de deelnemers,
e. de datum van inwerkingtreding en de geldingsduur van het convenant, en
f. de mogelijkheden van toetreding tot en opzegging van het convenant.

De regeling van taken en werkzaamheden, bedoeld onder a, dient tenminste een specifieke beschrijving te bevatten van de in § 4.6 genoemde typen van gegevensverwerking, voor zover het samenwerkingsverband deze typen uitvoert. Daarbij moet uitdrukkelijk worden getoetst of deze taken en werkzaamheden in voldoende mate samenhang vertonen met de taken van de deelnemende organisaties.

De regeling van de onder b bedoelde wijze waarop het samenwerkingsverband wordt bestuurd, kan onder meer regels bevatten over bijvoorbeeld een stuurgroep, bestaande uit vertegenwoordigers van de deelnemers, die de regie over de werkzaamheden van het verband

voert. De regeling zou ook – zie § 4.8 - een regisseur kunnen aanwijzen die de deelnemers ondersteunt bij de uitoefening van hun rol als gezamenlijk verantwoordelijke in de zin van de Wbp. In de regeling kan, tot slot, desgewenst gebruik worden gemaakt van de in § 4.8 genoemde mogelijkheid één van deelnemers als verantwoordelijke voor de gehele gegevensverwerking in het samenwerkingsverband aan te wijzen.

Bij de onder d bedoelde verplichtingen kan onder meer worden gedacht aan verplichtingen op het terrein van de bekostiging van de samenwerking, inclusief een eventueel ondersteunend bureau. Denkbaar is ook dat de verplichtingen betrekking hebben op het detacheren van medewerkers bij het bureau.

Met de aanwijzing in het convenant dat het samenwerkingsverband onder de werking van de kaderwet valt, vormt het samenwerkingsverband een publiekrechtelijke rechtsvorm. Er is immers sprake van een georganiseerd verband dat op basis van de kaderwet door middel van een convenant tot stand komt, waarbij de kaderwet de voorwaarden formuleert waaraan het samenwerkingsverband moet voldoen. Ook een eventueel bureau dat het samenwerkingsverband ondersteunt, kan als een publiekrechtelijke rechtsvorm worden aangemerkt, als dit op basis van de kaderwet door middel van het convenant in het leven wordt geroepen. Voor het zijn van een publiekrechtelijke rechtsvorm is het niet nodig dat het samenwerkingsverband of het bureau ook rechtspersoonlijkheid bezit.[102] Mocht voor een bepaald samenwerkingsverband aanleiding bestaan dit rechtspersoonlijkheid te geven, dan verdient de vorm van publiekrechtelijke rechtspersoonlijkheid de voorkeur. Daarvoor zal dan een specifieke wet nodig zijn. Onder omstandigheden is ook denkbaar dat een samenwerkingsverband de vorm van een privaatrechtelijke rechtspersoon krijgt. bijvoorbeeld die van stichting. Daartoe kan aanleiding bestaan bij deelname van private partijen. In dat geval is geen specifieke wet nodig. Omdat de kaderwet het samenwerkingsverband en een eventueel bureau tot publiekrechtelijke rechtsvormen zou maken, zou deze wet ook de basis kunnen bieden voor verstrekking van gegevens aan alle deelnemers van het samenwerkingsverband tegelijk en aan het bureau. Daarmee zou de vraag of verstrekking daaraan wel een voldoende juridische grondslag heeft, tot het verleden gaan behoren.

De kaderwet zou met betrekking tot het convenant tot slot kunnen bepalen dat het wordt gepubliceerd in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar wordt gemaakt.

4.4 Verplichte uitwisseling van gegevens

De deelname aan een samenwerkingsverband kan niet vrijblijvend zijn. De kaderwet zou dan ook moeten voorschrijven dat de deelnemers verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens aan de andere deelnemers te verstrekken, voor zover zij daarop geen uitzonderingen mogelijk hebben gemaakt. Benadrukt wordt dat deze verplichting alleen geldt voor noodzakelijke gegevens. Het noodzakelijkheidsvereiste, zoals dat uit het EVRM voortvloeit en in artikel 8 Wbp is neergelegd, blijft dus overeind.

De verplichting tot gegevensverstrekking in een kaderwet voor specifiek samenwerkingsverbanden zou als een "lex specialis" kunnen worden gezien ten opzichte van de generieke geheimhoudingsbepalingen in sectorwetten en zou aldus voorrang hebben boven die bepalingen. Om op dit punt echter geen misverstand te laten ontstaan verdient het de voorkeur in de kaderwet

---

[102] Samenwerkingsverbanden die onder de kaderwet vallen, kunnen in dit opzicht enigszins worden vergeleken met adviescolleges. Ook zij hebben geen rechtspersoonlijkheid. Wel worden zij aangemerkt als een publiekrechtelijke rechtsvorm. Het verschil met adviescolleges is dat de kaderwet voor samenwerkingsverbanden die onder die wet willen vallen, voorschrijft dat zij bij convenant worden opgericht, terwijl de huidige Kaderwet adviescolleges voorschrijft dat adviescolleges worden ingesteld bij wet. Voor het zijn van een publiekrechtelijke rechtsvorm doet dat verschil echter niet ter zake.

uitdrukkelijk te bepalen dat geheimhoudingsbepalingen in andere wetten buiten toepassing blijven. Daarmee kan een kaderwet knelpunten als omschreven in § 3.5 wegnemen.

Op de verplichting tot gegevensverstrekking en het buiten toepassing laten van geheimhoudingsbepalingen zou voorshands een uitzondering moeten worden gemaakt, voor zover het om bijzondere persoonsgegevens als bedoeld in artikel 16 Wbp zou gaan. Het gaat om gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakbond, en strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. De gevoelige aard van deze gegevens lijkt mee te brengen dat de verplichting tot gegevensverstrekking en het buiten toepassing laten van geheimhoudingsbepalingen – denk hierbij aan het medisch beroepsgeheim - in beginsel niet voor dergelijke gegevens geldt. Mocht er aanleiding bestaan om met betrekking tot (bepaalde categorieën van) dergelijke gegevens toch een bevoegdheid dan wel verplichting tot gegevensverstrekking aan bepaalde samenwerkingsverbanden in het leven te roepen, dan zal daarvoor een specifieke wettelijke grondslag nodig blijven.

Op het beginsel om de verplichting tot gegevensverstrekking en het buiten toepassing laten van de geheimhoudingsbepalingen niet op bijzondere persoonsgegevens betrekking te laten hebben, zou op zijn beurt tenminste één uitzondering moeten worden gemaakt. Deze uitzondering zou betrekking hebben op strafrechtelijke gegevens. Het betreft hier gegevens die bij uitstek relevant kunnen zijn voor samenwerkingsverbanden op het brede terrein van de in § 4.2 beschreven controletaak van de overheid. Om die reden is in § 3.7 dan ook bepleit de mogelijkheden om strafrechtelijke gegevens aan samenwerkingsverbanden te verstrekken, te verbeteren. Dat zou kunnen geschieden door in de Wpg en Wjsg bepalingen op te nemen die een algemene grondslag voor gegevensverstrekking aan samenwerkingsverbanden als bedoeld in de kaderwet geeft. Een dergelijke algemene grondslag zou impliceren dat het niet meer nodig zou zijn om voor ieder samenwerkingsverband afzonderlijk een basis voor gegevensuitwisseling in het Bpg en het Bjsg te leggen.

Een mogelijke andere uitzondering op voornoemd beginsel zou kunnen gelden voor persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Dergelijke gegevens kunnen immers relevant zijn voor samenwerkingsverbanden op het terrein van de handhaving van de openbare orde en veiligheid.

De verplichting tot gegevensverstrekking is ook anderszins niet absoluut. Partijen kunnen in het informatieprotocol (zie hierna § 4.10) uitzonderingen hierop opnemen. Een uitzondering moet zijn ingegeven door een belang bij de desbetreffende deelnemer dat zwaarder weegt dan het gezamenlijke belang van de deelnemers aan het samenwerkingsverband. Te denken valt aan een belang bij politie en OM om gegevens uit een lopend opsporingsonderzoek waarin een relatie met één van de andere deelnemers is te leggen, niet met die andere deelnemers te delen.

Onder de verplichting tot gegevensverstrekking zou ook de verstrekking aan politie, andere opsporingsdiensten en OM vallen. In § 3.6 is in dit verband bepleit dat gegevens in samenwerkingsverbanden voortaan aan de politie, andere opsporingsdiensten of het OM kunnen worden verstrekt, zonder dat daarvoor een vordering als bedoeld in artikel 126nc of 126nd WSv nodig is. Daartoe zou in het wetsvoorstel voor een kaderwet een wijziging van het Wetboek van Strafvordering moeten worden opgenomen met als strekking dat voor de verstrekking in een samenwerkingsverband van gegevens aan de politie, andere opsporingsdiensten of het OM een dergelijke vordering achterwege kan blijven. Mocht het onder omstandigheden zo zijn dat een bestuursorgaan onvoldoende kennis over de achtergrond van het desbetreffende verzoek bezit of andere redenen heeft om de verantwoordelijkheid en eventuele aansprakelijkheid voor de verstrekking van de gegevens niet te willen dragen, dan kan het gebruik maken van de hiervóór beschreven mogelijkheid in het informatieprotocol vast te leggen dat het van verstrekking kan afzien. In dat geval zal de politie, de opsporingsdienst of het OM buiten het samenwerkingsverband, zo nodig, alsnog een vordering op grond van artikel 126nc, respectievelijk 126nd kunnen instellen. Verder zou rekening moeten worden gehouden met eventuele wensen van deelnemers aan een samenwerkingsverband omtrent het gebruik dat opsporingsdiensten en OM

vervolgens van de ontvangen gegevens maken. Daaraan zou invulling kunnen worden gegeven door in een kaderwet te bepalen dat de deelnemers aan een samenwerkingsverband waaraan ook opsporingsdiensten en OM deelnemen, in het informatieprotocol (zie § 4.10) kunnen vastleggen dat gegevens die deze instanties zonder vordering verkrijgen, door hen alleen mogen worden gebruikt voor uitvoering van acties die zijn gebaseerd op adviezen die de gezamenlijke deelnemers in het kader van het samenwerkingsverband hebben opgesteld. De deelnemers zouden desgewenst in het informatieprotocol ook kunnen vastleggen dat, indien het OM mede op basis van de ontvangen gegevens een vervolging wil starten, deze gegevens daarvoor alleen mogen worden gebruikt als deze alsnog worden gevorderd.

4.5 Specifieke vastlegging van soorten gegevens

Uit een oogpunt van transparantie zou het wenselijk kunnen zijn in de kaderwet of een daaronder vallende AMvB aan te geven welke soorten van gegevens door de samenwerkingsverbanden kunnen worden gewisseld. Daarbij zou het de voorkeur verdienen dat bij AMvB te doen teneinde voldoende flexibel te kunnen inspelen op een eventueel behoefte de lijst van soorten gegevens aan te passen.

Voor zo'n lijst kan worden gedacht aan de volgende soorten van gegevens:
a. arbeidsgegevens, zijnde gegevens waarmee een door een persoon verrichte werkzaamheden vastgesteld kunnen worden;
b. gegevens inzake bestuursrechtelijke maatregelen en sancties, zijnde gegevens waaruit blijkt dat een natuurlijke persoon of een rechtspersoon een bestuursrechtelijke boete opgelegd heeft gekregen dan wel dat een andere bestuursrechtelijke maatregel is getroffen;
c. strafrechtelijke gegevens, zijnde gegevens als bedoeld in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens;
d. fiscale gegevens, zijnde gegevens waarmee de fiscale verplichtingen van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
e. gegevens roerende en onroerende goederen, zijnde gegevens waarmee het bezit en het gebruik van bepaalde goederen door een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
f. gegevens over uitsluitingsgronden van bijstand of uitkeringen, zijnde gegevens waaruit blijkt dat een persoon niet in aanmerking komt voor een uitkering;
g. handelsgegevens, zijnde gegevens waarmee de aard en werkzaamheden van een rechtspersoon kunnen worden vastgesteld;
h. huisvestingsgegevens, zijnde gegevens waarmee de (daadwerkelijke) verblijfs- of vestigingsplaats van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
i. identificerende gegevens, zijnde bij een natuurlijk persoon: naam, adres, woonplaats, postadres, geboortedatum, geslacht, burgerservicenummer en andere administratieve kenmerken en bij een rechtspersoon: naam, adres, postadres, rechtsvorm, vestigingsplaats en administratieve kenmerken;
j. inburgeringsgegevens, zijnde gegevens waarmee kan worden vastgesteld of aan een persoon inburgeringsverplichtingen zijn opgelegd;
k. nalevingsgegevens, zijnde gegevens waarmee de nalevingshistorie van wet- en regelgeving van een natuurlijk persoon of rechtspersoon kan worden vastgelegd;
l. onderwijsgegevens, zijnde gegevens waarmee de financiële ondersteuning ten behoeve van de bekostiging van onderwijs kan worden vastgesteld;
m. pensioengegevens, zijnde gegevens waarmee de pensioenrechten kunnen worden vastgesteld;
n. re-integratiegegevens, zijnde uitsluitend de gegevens waarmee kan worden vastgesteld of aan een persoon re-integratieverplichtingen zijn opgelegd en of deze worden nageleefd;
o. schuldenlastgegevens, zijnde gegevens waarmee de eventuele schulden van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
p. uitkerings-, toeslagen- en subsidiegegevens, zijnde gegevens waarmee de financiële ondersteuning van een natuurlijk persoon of rechtspersoon kan worden vastgesteld;
q. vergunningen en ontheffingen, zijnde gegevens waarmee kan worden bepaald voor welke activiteiten een natuurlijk persoon of rechtspersoon toestemming heeft gevraagd of verkregen;
r. zorgverzekeringsgegevens, zijnde uitsluitend de gegevens waarmee kan worden vastgesteld of een persoon is verzekerd voor de Zorgverzekeringswet;

s. gegevens over incidenten die hebben plaatsgevonden op het terrein van de openbare orde en veiligheid.

Wil deze lijst uit een oogpunt van transparantie en rechtszekerheid voldoende betekenis hebben, dan dient zij een limitatief karakter te hebben. Dat zou impliceren dat voor iedere soort van gegevens die in deze opsomming niet is genoemd maar ten aanzien waarvan in de praktijk zou gaan blijken dat zij relevant voor uitwisseling in samenwerkingsverbanden is, de AMvB aanpassing behoeft. Om op dit punt enige extra flexibiliteit te hebben, lijkt het wenselijk in de kaderwet de mogelijkheid te scheppen dat aanvulling van deze opsomming bij ministeriële regeling kan plaatsvinden.

De lijst is voor het overgrote deel ontleend aan artikel 5a.1, derde lid, Besluit Suwi. De opsomming in die bepaling dekt al nagenoeg volledig de soorten van gegevens die relevant kunnen zijn voor uitwisseling in samenwerkingsverbanden. Toegevoegd zijn de strafrechtelijke gegevens (onderdeel c). Deze toevoeging houdt verband met het pleidooi in § 3.7 om in de kaderwet voor alle samenwerkingsverbanden die onder de reikwijdte van die wet zouden vallen, de mogelijkheid tot verstrekking van strafrechtelijke persoonsgegevens te creëren, zodat het niet langer noodzakelijk is dat voor ieder samenwerkingsverband afzonderlijk in het Bpg en het Bjsg te regelen. Ook zijn toegevoegd de gegevens over incidenten die hebben plaatsgevonden op het terrein van de openbare orde en veiligheid (onderdeel s). Deze toevoeging houdt verband met de wens een eventuele kaderwet mede betrekking te laten hebben op gegevensuitwisseling ten behoeve van de handhaving van de openbare orde en veiligheid (zie § 4.2).

De kaderwet zou uit een oogpunt van transparantie ook kunnen expliciteren uit welke gegevensbronnen een samenwerkingsverband mag putten. Daarbij kan worden gedacht aan gegevens die afkomstig zijn:

a. van de deelnemers,
b. uit bij wet ingestelde openbare registers,
c. uit openbare bronnen,
d. uit registraties met authentieke gegevens,
e. van derden, voor zover dezen aannemelijk kunnen maken dat zij rechtmatig over deze gegevens beschikken.

Deze opsomming dekt in voldoende mate de bronnen die in de praktijk worden gebruikt, met dien verstande dat bij gebruik van gegevens, bedoeld onder e, de eis wordt gesteld dat de verstrekker van gegevens tegenover het samenwerkingsverband in voldoende mate aannemelijk moet maken dat hij rechtmatig over deze gegevens beschikt. Deze eis wordt niet alleen ingegeven door het belang van zorgvuldig overheidsoptreden, maar ook door het belang te voorkomen dat de verantwoordelijke voor de gegevensverwerking in het samenwerkingsverband aansprakelijk wordt gesteld voor de verwerking van gegevens die de betrokken derde onrechtmatig heeft verkregen.

4.6 Legitimatie typen van gegevensverwerking

Om de bestaande onduidelijkheid over welke typen van gegevensverwerking zijn toegestaan weg te nemen, wordt in § 3.8 aangegeven dat een kaderwet zou kunnen expliciteren dat de door deze kaderwet gereguleerde gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in die wet beschreven typen van gegevensverwerking. Deze beschrijving zou de volgende typen kunnen bevatten:

a. het opstellen van rapporten waarin inzichten worden geboden of trends worden gesignaleerd die voor het bereiken van het doel van het samenwerkingsverband relevant zijn,
b. het opstellen van adviezen over acties om het doel van het samenwerkingsverband te bereiken, en het uitvoeren daarvan,
c. het uitvoeren van analyses om de hiervóór bedoelde rapporten en adviezen te kunnen opstellen,
d. het opstellen van profielen van groepen van personen, organisatie of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien,
e. het koppelen van deze profielen aan gegevens waarover het samenwerkingsverband rechtmatig de beschikking heeft, teneinde een lijst te kunnen opstellen van personen,

organisaties of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien,

f. het signaleren van patronen en het opstellen van risico-indicatoren voor het uitvoeren van analyses en het opstellen van profielen, of

g. het delen van informatie, inzicht en kennis in andere dan de hiervóór bedoelde vormen, voor zover dat voor het bereiken van het doel van het samenwerkingsverband relevant is.

Voor deze opsomming van typen van verwerking is mede acht geslagen op bestaande vormen van gegevensverwerking in samenwerkingsverbanden en op nieuwe vormen daarvan die nog in ontwikkeling zijn, maar door bijvoorbeeld twijfel over de toelaatbaarheid daarvan onder de huidige wetgeving, in de praktijk nog niet worden toegepast.

Waar met de onder a bedoelde rapporten gedoeld wordt op documenten met een louter beschrijvend karakter, wordt ervan uitgegaan dat adviezen als bedoeld onder b aanbevelingen bevat, bijvoorbeeld met betrekking tot het uitvoeren van een gezamenlijke interventiestrategie. De acties waarop onderdeel b doelt, kunnen zijn opgenomen in zo'n interventiestrategie. Het zal primair gaan om acties van de deelnemers zelf. Daarbij kan het ook gaan om acties die eventuele private deelnemers aan het samenwerkingsverband kunnen uitvoeren om de naleving van wettelijke voorschriften te bevorderen of strafbare feiten te voorkomen. Zo kunnen bestuursrechtelijke en strafrechtelijke handhaving worden aangevuld met privaatrechtelijke handhaving. Denkbaar is dat een interventiestrategie ook acties omvat die door andere organisaties dan de deelnemers zullen moeten worden uitgevoerd. Met betrekking tot alle acties waarop het advies betrekking heeft, stelt onderdeel b buiten twijfel dat de verwerking van gegevens zich ook uitstrekt tot het uitvoeren van deze acties.

De onder c en d bedoeld analyses en profielen kunnen zelfstandige producten van een samenwerkingsverband zijn, maar uiteraard ook zijn geïntegreerd in de rapporten en adviezen die onder a en b zijn bedoeld.

De lijst, bedoeld onder e, kan het karakter van een zgn. zwarte lijst krijgen. De implicaties van plaatsing op en dergelijke lijst kunnen fors zijn. Om die reden is bij het opstellen van een dergelijke lijst extra zorgvuldigheid geboden. De checklist die het Cbp heeft opgesteld voor het opstellen van zwarte lijsten in bedrijven of bedrijfstakken, kan hierbij behulpzaam zijn.[103]

Opneming van deze opsomming in de kaderwet zou mede tot doel hebben buiten twijfel te stellen dat de onder a tot en met f genoemde typen van verwerking toelaatbaar zijn. Omdat opneming daarvan ook tot doel heeft een limitatieve opsomming van toelaatbare typen te geven, bevat onderdeel g een restcategorie, die enerzijds ruimte geeft voor andere vormen van verwerking, maar deze anderzijds wel uitdrukkelijk bindt aan het doel van het samenwerkingsverband.

De kaderwet zou daarnaast moeten bepalen dat samenwerkingsverbanden ten behoeve van het signaleren van patronen en het opstellen van risico-indicatoren bestanden kunnen koppelen die zijn geselecteerd op basis van veronderstelde relevantie voor het signaleren van deze patronen of het opstellen van deze indicatoren. Aldus zou de kaderwet ook op dit punt de bestaande twijfel met betrekking tot de toelaatbaarheid van bepaalde typen van gegevensverwerking kunnen wegnemen. Daarmee zou een expliciete basis ontstaan voor vormen van "datamining", waarbij een computer met behulp van geavanceerde software bepaalde patronen kan signaleren die van belang zijn voor het opstellen van risico-indicatoren. Het kan hierbij niet gaan om analyses op basis van ongericht verzamelde informatie; de kaderwet zou moeten voorschrijven dat het om analyses moet gaan op basis van gerichte selecties van bestanden. Uit een oogpunt van transparantie zou de kaderwet tevens moeten voorschrijven dat de selectie van bestanden op een voor het publiek toegankelijke wijze openbaar moet worden gemaakt.

4.7 Zorgvuldigheid bij verwerking

[103] Zie: http://www.cbpweb.nl/downloads_overig/checklist_zwarte_lijsten.pdf.

Wil een kaderwet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverbanden opleveren, dan zal deze kaderwet op grond van de overwegingen in § 2.6, 3.9 en 3.12 niet alleen een verbetering van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voorzieningen moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan.

Met het oog daarop is het wenselijk in de kaderwet de volgende voorzieningen te treffen, die deels al eerder aan de orde zijn gekomen:

a. De gegevensuitwisseling moet betrekking hebben op gegevens waarvan kan worden aangetoond dat de uitwisseling noodzakelijk is voor het doel van het samenwerkingsverband.
b. Een mogelijke aantasting van de belangen van de natuurlijke personen of rechtspersonen op wie de uitwisseling van gegevens betrekking heeft, mag niet onevenredig zijn in verhouding tot het doel dat met de uitwisseling wordt beoogd.
c. Het doel dat met de uitwisseling wordt beoogd, kan in redelijkheid niet op minder ingrijpende wijze voor de betrokken personen of rechtspersonen worden bereikt.
d. Gelet op de vereisten a tot en met c, vindt de verwerking van gegevens zo mogelijk versleuteld plaats, voor zover dat geen onredelijke inspanning vergt en geen nadelige invloed op de effectiviteit van het samenwerkingsverband heeft.
e. De onderbouwing van de wijze waarop bij een eventuele koppeling van bestanden de selectie van deze bestanden plaatsvindt, en de eventueel gehanteerde risico-indicatoren zijn openbaar gemaakt op een voor het publiek toegankelijke wijze, voor zover de openbaarmaking daarvan geen nadelige invloed op de effectiviteit van het samenwerkingsverband heeft.
f. Bij de verstrekking van gegevens aan andere deelnemers wordt, waar nodig en mogelijk, aangegeven wat de graad van juistheid en betrouwbaarheid van de gegevens is, en of de gegevens zijn gebaseerd op feiten dan wel een persoonlijk oordeel.[104]
g. Voordat de deelnemers aan het samenwerkingsverband tot verwerking van persoonsgegevens overgaan, voeren zij een zgn. "Privacy Impact Assessment" (PIA) uit.
h. De door de deelnemers aangewezen vertegenwoordigers die betrokken zijn bij de gegevensverwerking in het samenwerkingsverband, en de medewerkers van een eventueel ondersteunend bureau zijn verplicht tot geheimhouding van de door het samenwerkingsverband ontvangen en verder verwerkte persoonsgegevens en andere gegevens waarvan redelijkerwijs is aan te nemen dat bekendmaking daarvan de belangen van de deelnemers zou schaden, behoudens voor zover de realisering van het doel van het samenwerkingsverband tot bekendmaking daarvan noodzaakt.
i. De deelnemers voeren, behoudens spoedeisende gevallen, acties op grond van de uitgewisselde gegevens slechts uit na overleg met de deelnemers van wie de gegevens afkomstig zijn.
j. De deelnemers aan het samenwerkingsverband stellen een informatieprotocol vast waarin in ieder geval de in § 4.10 genoemde onderwerpen zijn geregeld.

De eisen onder a, b en c vloeien, voor zover zij op persoonsgegevens betrekking hebben voort uit artikel 8 EVRM. Daarin liggen het vereiste van noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit verankerd. Hoewel deze eisen al rechtstreekse gelding op basis van het EVRM hebben, lijkt het wenselijk deze in de kaderwet te expliciteren. Hiermee wordt benadrukt dat ook het gebruik van de ruimere mogelijkheden van gegevensverwerking die de kaderwet biedt, moet worden getoetst aan deze eisen.[105]

De eis onder d ziet op de toepassing van vormen van anonimisering en pseudonimisering. Waar dat met een redelijke inspanning mogelijk is, dienen dergelijke vormen conform het principe van "Privacy by Design" te worden ingepast in het proces van gegevensverwerking. Een goed

[104] Deze waarborg is ook terug te vinden in artikel 6 van het voorstel voor een Europese Richtlijn gegevensbescherming opsporing en vervolging van 25 januari 2012, COM(2012)10.
[105] De kaderwet volgt in dit opzicht dezelfde lijn als onlangs in het nieuwe artikel 5a.1, vierde lid, Besluit Suwi is neergelegd.

voorbeeld hiervan is de pseudonimisering die in het proces van gegevensverwerking met behulp van SyRI plaatsvindt. Dit proces houdt in dat aan de hand van gepseudonimiseerde gegevens en met behulp van vooraf bepaalde risico-indicatoren potentiële treffers worden bepaald ten aanzien van (gepseudonimiseerde) personen die een verhoogd risico laten zien dat zij fraude plegen. Op basis van dit "hit-no-hit"-systeem worden potentiële treffers vervolgens ontsleuteld voor een nader analyse op naam.[106]

De onder e opgenomen eis is bedoeld om processen van "datamining" en "profiling" een meer transparant karakter te geven. Juist bij dergelijke processen lijkt dat nodig om de uitkomst van dergelijke processen beter toetsbaar te doen zijn. De openbaarmaking op een voor het publiek toegankelijke wijze kan bestaan uit bijvoorbeeld publicatie op de website van het samenwerkingsverband.

Bij gegevensuitwisseling in samenwerkingsverbanden is het bij uitstek van belang dat de context waarbinnen een gegeven is verzameld of ontstaan, zo nodig en mogelijk wordt meegegeven aan de andere deelnemers aan het samenwerkingsverband. Met het oog daarop is de onder f beschreven eis opgenomen.[107]

Met het onder g bedoelde "Privacy Impact Assessment" (PIA) kan op gestructureerde en transparante wijze zichtbaar worden gemaakt wat de eventuele effecten van de gegevensuitwisseling voor de bescherming van persoonsgegevens zijn. Tijdens het proces waarin de PIA wordt uitgevoerd, kunnen bepaalde elementen van de gegevensuitwisseling zo nodig worden heroverwogen om tot een betere bescherming van persoonsgegevens te komen. De eis van een PIA vloeit voort uit het regeerakkoord.[108] Voor het uitvoeren van een PIA op rijksniveau heeft het kabinet een toetsmodel vastgesteld, dat sinds 1 september 2013 verplicht moet worden toegepast.[109]

Onderdeel h bevat een geheimhoudingsplicht met betrekking tot door het samenwerkingsverband ontvangen en verder verwerkte gegevens. Deze plicht is zo geformuleerd dat er ruimte blijft voor de deelnemers aan het samenwerkingsverband om gegevens, zo nodig, bekend te maken bij het uitvoeren van acties op grond van analyses en adviezen die het samenwerkingsverband heeft opgesteld.

Onder i is het "gazo"-principe vastgelegd. Opneming van dit principe moet – zie § 3.12 - bijdragen aan het vertrouwen dat deelnemers hebben in het gebruik van hun gegevens door andere deelnemers. Bij acties waaraan voorafgaand overleg moet plaatsvinden, kan worden gedacht aan bijvoorbeeld het stopzetten van een uitkering. Als het voorgenomen intrekken daarvan mede op gegevens van de politie wordt gebaseerd, kan overleg met de politie aanleiding zijn om bijvoorbeeld de intrekking uit te stellen, omdat dit in verband met een lopend politieonderzoek de voorkeur verdient.

4.8 Verantwoordelijke

Gelet op de verantwoordelijkheidstoedeling, zoals deze zich meestal in de praktijk voordoet, zou een kaderwet de deelnemers aan het samenwerkingsverband als gezamenlijk verantwoordelijke in de zin van de Wbp kunnen aanwijzen, tenzij zij in het convenant anders overeenkomen. Voor dat laatste kan aanleiding zijn, indien er sprake is van afzonderlijke verantwoordelijkheid per (deel)verwerking. Ook kan de situatie bestaan dat, ook al nemen aan de verwerkingen verschillende organisaties deel, er voor één gemeenschappelijke verantwoordelijke wordt gekozen. In dat geval zal die partij wel een dusdanige positie in het samenwerkingsverband dienen te hebben dat zij deze verantwoordelijkheid kan dragen. Anders gezegd: de duidelijkheid die de

---

[106] Vgl. kamerstukken 2012-2013, 33579, nr. 3, blz. 3 e.v. Zie ook artikel 5a.2 Besluit SUWI.
[107] Zie ook § 3.9, alsmede De Moor-van Vugt, a.w., blz. 75.
[108] Regeerakkoord VVD-PvdA van 29 oktober 2012, "Bruggen slaan", blz. 28.
[109] Kamerstukken II 2012-2013, 26643, nr. 282 herdruk.

keuze voor één verantwoordelijke biedt, mag niet ten koste gaan van de mate waarin aan deze verantwoordelijkheid invulling kan worden gegeven.

De gezamenlijke verantwoordelijkheid geldt uitsluitend voor de verwerking van gegevens binnen het samenwerkingsverband. De deelnemers zijn en blijven ieder voor zich verantwoordelijke in de zin van de Wbp voor het "voortraject", d.w.z. het verstrekken van gegevens aan het samenwerkingsverband.[110]

Het uitgangspunt dat partners gezamenlijk verantwoordelijke zijn, kan het risico meebrengen dat de partners hun verantwoordelijkheden onvoldoende onderkennen. Dit risico kan worden beperkt door een "regisseur" aan te wijzen die de partners ondersteunt in de uitoefening van hun rol als verantwoordelijke. De huidige praktijk kent hiervan reeds enkele voorbeelden.[111] Het gaat hier om een louter ondersteunende rol; zij neemt de gezamenlijke verantwoordelijkheid van de partners niet weg. In een eventuele kaderwet behoeft zij dan ook geen expliciete regeling.

4.9 Informatieplicht

In § 4.4 is aangegeven dat in de kaderwet wordt bepaald dat de deelnemers aan een samenwerkingsverband verplicht zijn de noodzakelijke gegevens aan dat samenwerkingsverband te verstrekken. Zoals in § 3.11 al is beschreven, maakt een dergelijke bepaling het mogelijk dat niet iedere betrokkene afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar. Op basis van de kaderwet en het op grond van die wet verplichte convenant en informatieprotocol (zie nader § 4.10) is in algemene zin al genoegzaam af te leiden welke gegevens ten behoeve van welk doel worden verwerkt. De kaderwet dient in verband daarmee voor te schrijven dat convenant en informatieprotocol worden gepubliceerd (zie §4.3 en 4.10). De kenbaarheid van de gegevensverwerking kan verder worden vergroot via de gebruikelijke voorlichtingsactiviteiten op websites en door middel van brochures.

4.10 Informatieprotocol

Uit een oogpunt van "accountability" is het wenselijk dat de kaderwet zal voorschrijven dat de deelnemers aan het samenwerkingsverband in een informatieprotocol een aantal elementen vastleggen die bij de gegevensverwerking in een samenwerkingsverband in het belang van gegevensbescherming van belang zijn. Omdat het hierbij niet alleen om persoonsgegevens kan gaan maar bijvoorbeeld ook om bedrijfsgegevens, wordt de term "informatieprotocol" in plaats van "privacyprotocol" gehanteerd.

De kaderwet zal moeten bepalen welke elementen dit informatieprotocol in ieder geval dient te bevatten. Daarbij kan worden gedacht aan de volgende elementen:
a. een beschrijving van de (soorten van) gegevens die worden uitgewisseld;
b. een verantwoording van de wijze waarop aan de eisen a tot en met g uit § 4.7 uitvoering is c.q. zal worden gegeven;
c. de inrichting van het proces van gegevensuitwisseling en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens;
d. uitzonderingen op de verplichting tot gegevensuitwisseling (zie § 4.4);
e. de beveiliging van de gegevens, met inbegrip van de autorisatie van personen die toegang tot de gegevens of aan te wijzen categorieën daarvan mogen hebben (art. 13 Wbp);
f. informatieverstrekking over de gegevensuitwisseling aan het publiek en aan betrokkenen;
g. de rechten van betrokkenen: inzage, correctie, verzet (artt. 35, 36, 40 Wbp);
h. verstrekking aan derden en de protocollering daarvan;
i. bewaartermijnen (art. 13 Wbp);
j. de verwijdering en vernietiging van bewaarde gegevens.

[110] Vgl. Kamerstukken II 2012-2013, 33579, nr. 3, blz. 37-38.
[111] Vgl. de regisseur die in artikel 10 Informatieprotocol FEC 2011 is aangewezen.

Op grond van onderdeel a zal het informatieprotocol een nadere aanduiding moeten geven van de soorten van gegevens uit de in § 4.5 opgenomen lijst die in het samenwerkingsverband zullen worden uitgewisseld.

Bij de inrichting van het proces van gegevensuitwisseling gaat het om een beschrijving van het proces van gegevensverwerking en van het eventuele gebruik van een informatiesysteem daarbij. Bij waarborgen voor de bescherming van persoonsgegevens die in de inrichting van het proces van gegevensuitwisseling zijn opgenomen, kan worden gedacht aan het hanteren van een getrapte vorm van gegevensuitwisseling (eerst "hit-no hit", pas bij voldoende hits uitwisseling van de inhoud van gegevens) en vormen van pseudonimisering.

Met betrekking tot onderdeel d kan worden opgemerkt dat een uitzondering op de verstrekkingsplicht zowel kan slaan op een individuele casus als op bepaalde, zeer bijzondere gegevens die in structurele zin niet aan het samenwerkingsverband worden verstrekt. Het doel van de regeling in het informatieprotocol moet zijn dat voor alle partijen vooraf helder is in welke gevallen op deze uitzonderingsmogelijkheid een beroep kan worden gedaan.

Bij informatieverstrekking aan het publiek (onderdeel f) kan worden gedacht aan informatieverstrekking over het doel van het samenwerkingsverband en de categorieën van gegevens die hiertoe worden uitgewisseld, op websites en in brochures. Het gaat hier om informatieverstrekking in aanvulling op de voorgeschreven openbaarmaking van het convenant en het informatieprotocol. Op grond van artikel 34, vijfde lid, Wbp is het niet nodig iedere persoon van wie in het samenwerkingsverband persoonsgegevens worden verwerkt, daarvan persoonlijk op de hoogte te stellen. Wel dient betrokkene op diens verzoek te worden geïnformeerd over het wettelijke voorschrift dat tot vastlegging of verstrekking van de desbetreffende gegevens heeft geleid. Uit onderdeel f vloeit voort dat het informatieprotocol ook daarover nadere regels dient te bevatten.

Voor de beveiliging van gegevens is het wenselijk in het informatieprotocol de richtsnoeren die het Cbp daartoe heeft opgesteld, als uitgangspunt te nemen.[112]

Het informatieprotocol zou ter uitvoering van onderdeel h kunnen bepalen dat doorverstrekking aan een derde (met inbegrip van een ander samenwerkingsverband) alleen plaatsvindt met toestemming van de partner van wie de gegevens oorspronkelijk afkomstig zijn.

Het gaat hier om een niet-uitputtende opsomming: de deelnemers aan het samenwerkingsverband kunnen desgewenst andere elementen aan het informatieprotocol toevoegen.

De kaderwet zou met betrekking tot het informatieprotocol tot slot kunnen bepalen dat het wordt gepubliceerd in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar wordt gemaakt.

4.11 Rechtsbescherming en toezicht

Een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden zou een aanvulling vormen op de bestaande wetgeving met betrekking tot verwerking van persoonsgegevens. Dat impliceert dat de bestaande rechten van personen omtrent wie een samenwerkingsverband gegevens verwerkt, onverkort in stand blijven. Dat geldt voor rechten als het inzagerecht, het correctierecht en het recht van verzet, zoals geregeld in onderscheidenlijk de artikelen 35, 36 en 40 Wbp of daarmee vergelijkbare rechten in specifieke wetgeving (vgl. artt. 25 en 28 Wpg en 18, 22 en 26 Wjsg).

Burgers dienen over voldoende informatie te beschikken om te kunnen beoordelen of voor hen aanleiding bestaat deze rechten uit te oefenen. Nu een kaderwet – zie § 4.9 – het mogelijk zou

[112] Zie Stcrt. 2013, 5174.

maken dat niet iedere betrokken burger afzonderlijk zou moete worden geïnformeerd over de verwerking van gegevens over hem of haar, is het van belang dat een burger wel anderszins voldoende in staat is te voorzien of zijn of haar gegevens worden verwerkt. Deze voorzienbaarheid zal in de eerste plaats kunnen blijken uit de kaderwet zelf, de parlementaire stukken over deze wet, het convenant en het informatieprotocol. Van belang daarbij is dat convenant en protocol gepubliceerd moeten worden. De kenbaarheid van de gegevensverwerking zal verder worden vergroot door de regels die het samenwerkingsverband in het informatieprotocol moet vastleggen over de informatieverstrekking aan het publiek en aan betrokkenen. Afhankelijk van het doel van het samenwerkingsverband, is het wenselijk in het informatieprotocol te bepalen dat personen ten aanzien van wie het voornemen bestaat een bepaalde interventie te plegen, in beginsel informatie wordt verschaft omtrent de gegevensverwerking die aan de voorgenomen interventie ten grondslag ligt. Dat vergroot in belangrijke mate de transparantie van het doel en de aard van de gegevensverwerking voor de betrokken burger. Het protocol zou kunnen bepalen dat op dit beginsel alleen uitzondering wordt gemaakt, indien in het protocol genoemde gronden daartoe aanleiding geven. Daarbij kan worden gedacht aan gronden die in artikel 43 Wbp worden genoemd.[113] Het lijkt niet doenlijk dergelijke regels ook in de kaderwet zelf vast te leggen, nu het sterk afhangt van het specifieke samenwerkingsverband of dit al dan niet adviezen over te plegen interventies afgeeft en, zo ja, in welke mate en onder welke voorwaarden betrokkenen geïnformeerd kunnen worden over de gegevensverwerking die daaraan ten grondslag ligt. Dat vereist maatwerk in het informatieprotocol. Van belang is wel dat met het oog op de belangen van betrokkenen informatieverstrekking in vorenbedoelde zin als uitgangspunt wordt genomen.

Aan de transparantie van de gegevensverwerking en daarmee aan de aanspreekbaarheid van het samenwerkingsverband op een zorgvuldige verwerking ("accountability") wordt verder bijgedragen door een aantal waarborgen die een aanvulling vormen op de waarborgen in de bestaande privacywetgeving. Het betreft in de eerste plaats de verplichting om de onderbouwing van de wijze waarop bij een eventuele koppeling van bestanden de selectie van deze bestanden plaatsvindt, en de eventueel gehanteerde risico-indicatoren op een voor het publiek toegankelijke wijze openbaar te maken (zie § 4.7). Verder valt te wijzen op de elementen die in § 4.10 worden genoemd als verplichte elementen van een op te stellen en openbaar te maken informatieprotocol. Weliswaar is de wijze waarop deze elementen precies worden ingevuld, een kwestie van maatwerk per samenwerkingsverband, maar het enkele feit dat deze elementen regeling vergen, draagt ontegenzeggelijk bij aan de transparantie van de gegevensverwerking.

Naast de bestaande rechten van de betrokken burger en de voorzieningen in de kaderwet die de transparantie van de gegevensverwerking kunnen vergroten, kan de kaderwet ook waarborgen bevatten die anderszins aan de bescherming van persoonsgegevens bijdragen. Het gaat om waarborgen, zoals die in § 4.7 zijn beschreven. De belangrijkste daarvan is wellicht de verplichting om een " Privacy Impact Assessment" (PIA) uit te voeren. Een dergelijke verplichting bestaat nu alleen op grond van een kabinetsbesluit voor het rijksniveau, maar zal in de kaderwet een wettelijke verankering voor gegevensuitwisseling in samenwerkingsverbanden krijgen en tevens gaan gelden voor deelnemers uit de kring van de medeoverheden en private partijen.

Voorts gelden uiteraard de waarborgen voor de bescherming van persoonsgegevens, zoals die in de Wbp zijn neergelegd. Dat geldt ook voor verstrekking aan derden in landen buiten de Europese Unie, waarbij de artikelen 75 tot en met 78 Wbp in acht moeten worden genomen.

[113] Ingevolge artikel 43 Wbp kan een verantwoordelijke voor de gegevensverwerking de informatieverplichtingen, bedoeld in artikel 34 Wbp, buiten toepassing laten, voor zover dit noodzakelijk is in het belang van o.a. de voorkoming, opsporing en vervolging van strafbare feiten en het toezicht op de naleving van wettelijke voorschriften. Omdat artikel 34 Wbp al buiten toepassing kan blijven op grond van het vijfde lid van dat artikel (zie § 3.11), heeft artikel 43 Wbp in dit verband in eerste instantie geen relevantie. Dat neemt niet weg dat de gronden die in dat artikel worden genoemd om informatieverstrekking aan betrokkenen achterweg te laten, wel bruikbaar zijn voor het formuleren van gronden om een uitzondering te kunnen maken op een in het informatieprotocol vast te leggen informatieverplichting.

Aan de bescherming van persoonsgegevens draagt, tot slot, ook het houden van toezicht bij. Met het oog daarop is overwogen of in de kaderwet een verplichting zou moeten worden opgenomen om periodiek een zgn. privacy audit[114] uit te voeren. Uitvoering daarvan kan immers bijdragen aan de bescherming van persoonsgegevens. Voor sommige grote organisaties als de politie is een privacy audit voorgeschreven (vgl. art. 33 Wpg). Het lijkt echter te ver voeren een dergelijke verplichting ook voor samenwerkingsverbanden die onder de kaderwet vallen, in te voeren. Verschillende samenwerkingsverbanden zullen een te kleine schaal hebben om de lasten die een dergelijke verplichting meebrengt, te kunnen dragen. Het staat grotere samenwerkingsverbanden echter vrij om in een informatieprotocol de verplichting vast te leggen dat periodiek een privacy audit wordt uitgevoerd.

Extern toezicht vindt plaats door het College bescherming persoonsgegevens (Cbp). Ingevolge artikel 51 Wbp houdt het Cbp toezicht op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Deze taak is niet beperkt tot het terrein van de Wbp, maar strekt zich ook uit tot andere wetten, AMvB's en andere wettelijke regelingen op grond waarvan persoonsgegevens worden verwerkt. Dat geldt dus ook voor wetten waarin in aanvulling op de Wbp nadere regels zijn gesteld.[115] Dit impliceert dat de verwerking van persoonsgegevens onder de werking van een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden onder toezicht van het Cbp plaatsvindt.

4.12 Verhouding tot bestaande wetgeving

In § 4.1 is als uitgangspunt gekozen voor een opzet van een kaderwet gekozen waarbij de Wbp, de Wpg, de Wjsg en de bepalingen over gegevensverwerking in sectorale wetten, op mogelijk een enkele kleine aanpassing na, in stand blijven. In deze opzet zal een kaderwet een aanvulling op deze wetten vormen, voor zover het om gegevensuitwisseling in samenwerkingsverbanden gaat.

Dit impliceert dat bepalingen uit die wetten over verstrekking van gegevens aan derden, ook in relatie tot samenwerkingsverbanden die onder de werking van de kaderwet vallen, hun betekenis blijven houden, tenzij een specifieke bepaling uit de kaderwet deze buiten toepassing verklaart. Een voorbeeld van een bepaling die haar betekenis blijft houden, is artikel 32, eerste lid, onder f, Wpg, waarin is vastgelegd dat de politie de verstrekking van politiegegevens aan derden schriftelijk vastlegt (protocolplicht). Een voorbeeld van bepalingen die de kaderwet in relatie tot samenwerkingsverbanden buiten toepassing zou verklaren, zijn de geheimhoudingsbepalingen in andere wetten, tenzij het om geheimhouding gaat van bijzondere persoonsgegevens anders dan strafrechtelijke gegevens (zie § 4.4). Een essentiële aanvulling die de kaderwet met betrekking tot de verstrekking van gegevens bevat, is de verplichting tot verstrekking van de noodzakelijke gegevens aan het samenwerkingsverband, voor zover daarop in het informatieprotocol geen uitzondering wordt gemaakt.

De bepalingen in de kaderwet over de verdere verwerking van gegevens in en door het samenwerkingsverband geven ten opzichte van de bestaande wetgeving vooral een aantal aanvullende randvoorwaarden waaronder deze verwerking mag plaatsvinden. Het gaat om randvoorwaarden die deels een legitimerend karakter hebben, zoals de bepalingen die een nadere duiding geven van toelaatbare typen van gegevensverwerking (zie § 4.6). Andere randvoorwaarden hebben een meer normerend karakter, zoals de bepalingen met waarborgen voor een zorgvuldige gegevensverwerking en de bepalingen over de inhoud van het convenant en het informatieprotocol (zie respectievelijk § 4.7, 4.3 en 4.10). Ook voor deze fase van gegevensverwerking gaat het om aanvullende bepalingen. Zo blijven de bepalingen in de bestaande wetgeving waarin de rechten van betrokkenen worden geregeld (recht op inzage en correctie en recht van verzet), onverkort in stand hangt. Welke wetgeving in dit verband geldt, hangt, zoals ook nu al het geval is, af van het antwoord op de vraag of aan het samenwerkingsverband gegevens als bedoeld in de Wpg en Wjsg worden verstrekt, en of deze

---

[114] Zie het Raamwerk privacy audit (http://www.cbpweb.nl/Pages/ind_wetten_zelfr_compliance_rpa.aspx).
[115] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 177.

binnen dat verband op geautomatiseerde wijze worden verwerkt dan wel, voor zover dat niet het geval is, in een apart bestand worden opgeslagen.[116] Is dat niet het geval, dan gelden de rechten, zoals neergelegd in de Wpg (artt. 25 en 28) en Wjsg (artt. 18, 22 en 26). Is dat wel het geval, dan gelden de rechten die in de Wbp zijn vastgelegd (artt. 35, 36 en 40)

In § 4.1 is al naar voren gekomen dat de kaderwet ook als een algemene aanvulling kan worden gezien op wettelijke regelingen die in specifieke gevallen samenwerking voorschrijven en daarbij regels over gegevensuitwisseling geven, zoals de in artikel 9 van de Wet Suwi voorgeschreven samenwerking tussen het UWV, de SVB en de gemeenten bij de uitvoering van die wet en enige andere wetten. Deze specifieke wettelijke regelingen blijven uiteraard onverkort hun gelding houden. Hetzelfde geldt met betrekking tot wetten die een specifiek regime bevatten voor gegevensverwerking die tot een bepaald product moet leiden. Hierbij kan in de eerste plaats worden gedacht aan de Wet Bibob, die een specifieke regeling van de gegevensverwerking bevat die tot een Bibob-advies moet leiden.[117] Een ander voorbeeld van zo'n regime is de Wcr. Ook die wet bevat een specifieke regeling van de gegevensverwerking die tot een zgn. risicomelding met betrekking tot een rechtspersoon moet leiden. Het kan uiteraard niet zo zijn dat de specifieke waarborgen die dergelijke wetten kennen om gegevens tot bepaalde producten te verwerken, te niet te doen door een samenwerkingsverband onder de kaderwet op te richten met het doel op eenvoudigere wijze tot dezelfde producten te komen.

Hoewel de kaderwet primair een aanvullend karakter zou hebben, zou het in het licht van deze verkenning wenselijk c.q. noodzakelijk zijn in het voorstel voor een kaderwet ook enkele aanpassingen van bestaande wetten mee te nemen.

Een eerste aanpassing die in dit verband kan worden genoemd, betreft artikel 20 Wpg. Dit artikel vormt één van de zeer weinige artikelen waarin over een samenwerkingsverband wordt gesproken. Op grond van dit artikel kan de korpschef van de nationale politie in overeenstemming met het bevoegd gezag bepaalde politiegegevens aan samenwerkingsverbanden verstrekken, voor zover dat noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor de volgende doeleinden:
a. het voorkomen en opsporen van strafbare feiten,
b. het handhaven van de openbare orde,
c. het verlenen van hulp aan hen die deze behoeven,
d. het uitoefenen van toezicht op de naleving van regelgeving.

Gelet op § 4.2 zou de verstrekking voor de doeleinden a, b en d voortaan door de kaderwet worden bestreken. De korpschef behoeft voor die doeleinden geen overeenstemming met het bevoegd gezag meer te zoeken en niet te toetsen of er sprake is van een zwaarwegend algemeen belang. Die laatste toets ligt als het ware al opgesloten in de kaderwet. Om die reden zou overwogen kunnen worden artikel 20 Wpg zo aan te passen dat de in dat artikel geregelde mogelijkheid van gegevensverstrekking alleen nog maar betrekking heeft op verstrekking voor het verlenen van hulp aan hen die deze behoeven.

Een andere bepaling waarin over samenwerkingsverbanden wordt gesproken, is artikel 22, zesde lid, Wbp. Deze bepaling geeft ruimte om gegevens die op basis van artikel 20 Wpg of artikel 39f Wjsg aan een deelnemer aan een samenwerkingsverband zijn verstrekt, door deze deelnemer in het kader van een (ander) samenwerkingsverband kunnen worden doorverstrekt aan een andere organisatie. Deze bepaling kan komen te vervallen, omdat de kaderwet deze ruimte ook zal bieden.

---

[116] Vgl. ABRvS 16-7-2014, ECLI:NL:RVS:2014:2594.

[117] De Wet Bibob bevat niet alleen een specifieke regeling van gegevensverwerking die tot inzet van het Bibob-instrumentarium kan leiden. In deze wet komt ook een verwijzing voor naar de RIEC's als samenwerkingsverbanden waaraan gegevens mogen worden verstrekt, voor zover dat noodzakelijk is voor het ondersteunen van een bestuursorgaan of een rechtspersoon met een wettelijke taak bij het toepassen van die wet (artikel 28, tweede lid, onder d).

Buiten deze bepalingen bestaan op het niveau van wetgeving in formele zin geen bepalingen over samenwerkingsverbanden die mogelijk wijziging behoeven.[118] Wel komen dergelijke bepalingen in lagere regelgeving voor. Gedacht kan worden aan artikel 43c, eerste lid, onder m, van de Uitvoeringsregeling Awr. Als het tot indiening van een voorstel voor een kaderwet komt, zal te zijner tijd moeten worden bezien of deze en andere bepalingen op het niveau van lagere regelgeving aanpassing behoeven.

Tot slot zijn er nog enkele andere aanpassingen van wetten nodig. Het betreft in de eerste plaats een aanpassing van de Wpg en Wjsg met het doel daarin een algemene grondslag voor verstrekking van politiegegevens, onderscheidenlijk justitiële en strafvorderlijke gegevens aan samenwerkingsverbanden mogelijk te maken, voor zover deze onder de werking van de kaderwet vallen. Met een dergelijke grondslag is het niet meer nodig per individueel samenwerkingsverband een grondslag in deze wetten of in het Bpg c.q het Bjsg te creëren. Verder is een aanpassing van de artikelen 126nc en 126nd van het WSv nodig die ertoe strekt dat het niet langer nodig is een vordering tot verkrijging van gegevens in te stellen, als het om een verkrijging binnen een onder de kaderwet vallend samenwerkingsverband gaat.

4.13 Betekenis voor bestaande samenwerkingsverbanden

In § 4.1 is al naar voren gebracht dat de kaderwet niet tot doel heeft een exclusief regime voor gegevensuitwisseling in samenwerkingsverbanden te creëren. Het staat bestaande samenwerkingsverbanden dan ook vrij ervoor te kiezen hun gegevensverwerking in te blijven richten op grond van de thans al geldende wetgeving. Daartoe kan aanleiding bestaan, indien de kaderwet voor een samenwerkingsverband, gelet op haar behoeften aan informatie, niet of nauwelijks betere mogelijkheden tot gegevensuitwisseling boven de bestaande wetgeving biedt.

Indien de deelnemers aan een bestaand samenwerkingsverband wèl aanleiding zien onder de werking van de kaderwet te willen vallen, dan zal daarvan eerst sprake kunnen zijn, indien het samenwerkingsverband aan alle randvoorwaarden voldoet die de kaderwet daarvoor stelt. Het gaat daarbij in de eerste plaats om het voldoen aan de waarborgen die in § 4.7 zijn genoemd. Verder valt te denken aan het opstellen van een convenant en van een informatieprotocol dan wel het aanpassen van een bestaand convenant of informatieprotocol die aan de voorwaarden voldoen die in § 4.3 onderscheidenlijk 4.10 zijn genoemd. Pas als aan voorwaarden als deze is voldaan, kan in het convenant ook worden vastgelegd dat het samenwerkingsverband onder de werking van de kaderwet valt.

4.14 Toetsing aan het EVRM

De vraag kan rijzen hoe de kaderwet zich verhoudt tot het recht op bescherming van persoonsgegevens, zoals dat geregeld is in artikel 8 EVRM. Het eerste lid van dat artikel beschermt het recht op respect voor het privéleven. Dit recht is echter niet absoluut. Ingevolge het tweede lid van artikel 8 EVRM is een inmenging in de uitoefening van dit recht evenwel slechts gerechtvaardigd, wanneer de inmenging bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Het toezicht op de naleving van wettelijke voorschriften draagt, afhankelijk van de inhoud van deze voorschriften, bij aan het economisch welzijn van ons land, de bescherming van de gezondheid of de goede zeden en aan de bescherming van de rechten en vrijheden van burgers.

[118] Weliswaar wordt in 56 wetten over samenwerkingsverbanden gesproken, maar in alle andere gevallen dan de Wpg en Wbp gaat het om samenwerkingsverbanden die niet een zgn. controletaak van de overheid uitvoeren.

De handhaving van de openbare orde en veiligheid dient de openbare veiligheid en het voorkomen van wanordelijkheden. De voorkoming, opsporing en vervolging van strafbare feiten staat in het teken van het voorkomen van strafbare feiten. Daarmee worden alle doeleinden waarbinnen het meer specifieke doel van een samenwerkingsverband moet vallen, afgedekt door de doeleinden die artikel 8 EVRM noemt.

De eis uit artikel 8 EVRM dat de inmenging in de uitoefening van het recht op respect voor het privéleven bij wet moet zijn voorzien, houdt in dat er sprake is van een wettelijke basis die voor de burger voldoende toegankelijk en voorzienbaar is.[119] Aan deze eis wordt voldaan met de in deze paragraaf beschreven kaderwet en de daarop berustende bepalingen in een AMvB en ministeriële regeling, die gepubliceerd worden in het Staatsblad, respectievelijk de Staatscourant. Aan de toegankelijkheid draagt bij wat uit de parlementaire stukken over een kaderwet als toelichting op deze wet kan worden afgeleid. De voorzienbaarheid neemt verder toe door de in de kaderwet opgenomen verplichtingen om bepaalde onderwerpen in het convenant en het informatieprotocol nader te regelen en deze te publiceren in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar te maken.

De eis dat de inmenging noodzakelijk is in een democratische samenleving, wordt in de jurisprudentie van het EVRM nader ingevuld met het vereiste van een dringende maatschappelijke behoefte ("pressing social need"). Of hiervan sprake is, wordt bepaald aan de hand van een aantal criteria. Zo moet een maatregel om noodzakelijk te zijn, relevant zijn om het beoogde doel te bereiken en verder moet voldaan zijn aan het proportionaliteits- en het subsidiariteitsvereiste. In algemene zin kan worden gesteld dat samenwerkingsverbanden op de terreinen die de kaderwet beslaat, effectiever en efficiënter kunnen opereren, als zij gegevens kunnen uitwisselen. Sterker nog, de primaire aanleiding om een samenwerkingsverband aan te gaan, is veelal gelegen in de behoefte aan gegevensuitwisseling. Of de gegevensverwerking in een samenwerkingsverband ook in een concreet geval aan de hier genoemde vereisten voldoet, zal moeten worden getoetst bij de oprichting van het samenwerkingsverband en de inrichting van het proces van gegevensverwerking. De kaderwet zal expliciet voorzien in de verplichting de gegevensverwerking te toetsen aan het noodzakelijkheidsvereiste en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit.

4.15 Toetsing aan regelgeving van de EU

Een kaderwet die een opzet kent als in de voorgaande paragrafen beschreven, past binnen de voorschriften van de Europese privacyrichtlijn. De in de kaderwet geregelde verwerking van persoonsgegevens kan worden gebaseerd op twee gronden uit deze richtlijn.

De eerste grond is te vinden in artikel 7, onder d, van de richtlijn. Daarin is bepaald dat lidstaten de verwerking van persoonsgegevens mogen toestaan, indien deze verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke is onderworpen. Deze bepaling is terug te vinden in artikel 8, onder c, Wbp. Nu in § 4.4 wordt voorgesteld in de kaderwet voor te schrijven dat deelnemers aan een samenwerkingsverband verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens te verstrekken, wordt aan deze voorwaarde voldaan. Daarmee zal ook worden voldaan aan artikel 6, eerste lid, onder c, en derde lid, van het voorstel voor een Algemene verordening gegevensbescherming[120], waarin deze voorwaarde terugkomt. Weliswaar is de activering van deze verplichting afhankelijk van een besluit van de deelnemer om aan het desbetreffende samenwerkingsverband deel te nemen, maar dat doet niet af aan het verplichte karakter van de gegevensverstrekking op zich.

De tweede grond is gelegen in artikel 7, onder e, van de richtlijn. Ingevolge dat onderdeel mogen lidstaten de verwerking van persoonsgegevens toestaan, indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. Met de combinatie van het doel van de

---

[119] EHRM 26 april 1979 (Sunday Times), NJ 1980, 146.
[120] Zie de tekst van 25 januari 2012, COM(2012)11.

gegevensuitwisseling en het noodzakelijkheidsvereiste, zoals in § 4.2, respectievelijk § 4.7 zijn beschreven, wordt aan deze voorwaarde voldaan. Daarmee zal ook worden voldaan aan artikel 6, eerste lid, onder e, en derde lid, van het voorstel voor een Algemene verordening gegevensbescherming, waarin deze voorwaarde terugkomt. De desbetreffende voorwaarde is destijds geïmplementeerd in artikel 8, onder e, Wbp. In dat onderdeel heeft een precisering plaatsgevonden tot gegevensverwerking die noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt. Daarmee valt gegevensverwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang in de vorm van gegevensuitwisseling met private partijen, buiten dat onderdeel. Een kaderwet zal in zoverre een aanvulling op dat onderdeel geven dat zij – binnen de voorwaarde uit de Europese privacyrichtlijn - ook een wijze van gegevensuitwisseling met private partijen mogelijk maakt die – zie § 3.3 - de Wbp nu niet toelaat.

In § 3.4 is naar voren gekomen dat er verandering lijkt te komen in de omstandigheid dat de Europese privacyregelgeving weinig tot geen ruimte laat voor verdere verwerking van persoonsgegevens voor een doel dat niet verenigbaar is met het doel waarvoor zij zijn verzameld. Als het huidige voorstel voor een Algemene verordening gegevensbescherming wordt aangenomen, zal er meer ruimte ontstaan om bij onverenigbaarheid van doelen in een samenwerkingsverband toch tot gegevensuitwisseling over te gaan. Bij de voorbereiding van een eventuele kaderwet zal hiermee rekening moeten worden gehouden.

De verstrekking van strafrechtelijke persoonsgegevens door politie en OM aan een samenwerkingsverband valt in de toekomst onder de nieuwe Richtlijn gegevensbescherming opsporing en vervolging. Ingevolge artikel 7, aanhef en onder a, van het voorstel voor deze richtlijn[121] dienen lidstaten te bepalen dat het verwerken van strafrechtelijke persoonsgegevens die onder de werking van deze richtlijn vallen, slechts rechtmatig is wanneer en voor zover die verwerking noodzakelijk is voor – onder meer – het uitvoeren van een taak door een bevoegde autoriteit, op grond van een wettelijke bepaling, voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Deze bepaling geeft voldoende ruimte om door middel van de kaderwet verstrekking van strafrechtelijke persoonsgegevens door politie en OM aan een samenwerkingsverband mogelijk te maken, voor zover het om het voorkomen, opsporen en vervolgen van strafbare feiten gaat. Voor zover het om de overige doeleinden van de kaderwet gaat, zal een beroep kunnen worden gedaan op artikel 7, aanhef en onder b, van het voorstel voor die richtlijn. Daarin is, in navolging van de Europese privacyrichtlijn, bepaald dat lidstaten dienen voor te schrijven dat verwerking van strafrechtelijke persoonsgegevens die onder de werking van deze richtlijn vallen, slechts rechtmatig is wanneer en voor zover de verwerking noodzakelijk is om – onder meer – een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke is onderworpen. Bij die grond geldt dezelfde redenering als hiervóór met betrekking tot artikel 7, onder d, van de Europese privacyrichtlijn is gegeven.

[121] Zie de tekst van 25 januari 2012, COM(2012)10.

5. Slotbeschouwing

Een kaderwet gegevensuitwisseling samenwerkingsverbanden zal vooral tot doel moeten hebben om bestaande knelpunten in de gegevensuitwisseling weg te nemen en een aantal waarborgen voor een zorgvuldige gegevensverwerking vast te leggen. Die knelpunten betreffen zowel onduidelijkheden die de bestaande wetgeving in de toepassing op samenwerkingsverbanden meebrengt en die vanwege hun soms hardnekkige karakter niet met louter voorlichting zijn weg te nemen, als ook beperkingen die uit deze wetgeving voortvloeien. Beperkingen, zoals geheimhoudingsbepalingen, waaraan in algemene zin een grote waarde moet worden toegekend, maar die in relatie tot samenwerkingsverbanden tot onnodige belemmeringen leiden.

Een kaderwet kan dergelijke onduidelijkheden en belemmeringen wegnemen. Het betreft in de eerste plaats een betere legitimering van de verstrekking van gegevens aan de deelnemers en een eventueel bureau van een samenwerkingsverband en van de uitwisseling met private partijen. De kaderwet zal verder praktische barrières slechten om binnen een samenwerkingsverband gegevens aan politie en OM te verstrekken. Omgekeerd zal gaan gelden dat strafrechtelijke gegevens voortaan gemakkelijker door politie en OM aan de andere partners in een samenwerkingsverband kunnen worden verstrekt. De kaderwet zal ook een expliciete legitimatie geven aan gegevensverwerking in de vorm van "datamining" en "profiling" om daarmee de mogelijkheden voor de opbouw van "intelligence" te verbeteren. De kaderwet zal – tot slot – de noodzaak wegnemen om iedere persoon van wie gegevens worden verwerkt, daarvan afzonderlijk op de hoogte brengen, zonder dat daarvoor, zoals nu is vereist, de vraag moet worden beantwoord of dat een onevenredige inspanning zou vergen.

Los van het wegnemen van onduidelijkheden en belemmeringen kan een kaderwet richting en steun geven aan initiatieven die worden ontplooid om tot gegevensuitwisseling te komen, maar nu vanwege die onduidelijkheden en belemmeringen soms nog stranden of vergen dat opnieuw het wiel moet worden uitgevonden. Ook kan met een kaderwet het signaal worden afgegeven dat er meer mogelijk is dan wordt verondersteld.

Tegenover betere mogelijkheden tot gegevensverwerking staan ook betere waarborgen voor een zorgvuldige verwerking. De kaderwet zal een aantal belangrijke beginselen met betrekking tot de bescherming van persoonsgegevens expliciteren als toetssteen voor een geoorloofde gegevensverwerking. Te denken valt aan het vereiste dat aangetoond moet kunnen worden dat de gegevensverwerking noodzakelijk is en voldoet aan de beginselen van proportionaliteit en subsidiariteit. Andere vereisten zijn het versleutelen van gegevens waar dat met een redelijke inspanning mogelijk is en de effectiviteit niet onevenredig beïnvloedt, het openbaar maken van bijvoorbeeld eventuele risico-indicatoren die men gebruikt, en het uitvoeren van een "Privacy Impact Assessment". Zo kan een kaderwet een goede optelsom laten zien van betere mogelijkheden tot gegevensuitwisseling en de nodige waarborgen voor een zorgvuldige gegevensverwerking.

De werkgroep sluit deze verkenning graag af met de opmerking dat zij niet de pretentie heeft met deze verkenning alles tot in detail te hebben doordacht, maar wèl de overtuiging dat de verkenning een voldoende basis geeft om een positieve beslissing over het opstellen van een voorstel voor een kaderwet te kunnen nemen.

***Bijlage 1* Overzicht samenwerkingsverbanden**

SAMENWERKING	BETROKKEN PARTIJEN	DOEL/ TOELICHTING
Financieel Expertise Centrum (FEC)	DNB, AFM, Belastingdienst, FIU-Nederland, FIOD, Nationale Politie en OM. Voor specifieke activiteiten kunnen andere partijen deelnemen.	Versterken integriteit financiële sector.
Regionale Informatie- en Expertise Centra (RIEC's)	Gemeenten, provincies, Belastingdienst, Douane, Inspectie SZW, Nationale Politie, FIOD, KMAR, IND en OM.	Versterken en ondersteunen bestuurlijke en geïntegreerde aanpak van georganiseerde en ondermijnende criminaliteit.
Regionale Coördinatiecentra Fraudebestrijding (RCF's)/ Landelijke Interventieteams	Belastingdienst, Inspectie SZW, UWV, gemeente, SVB, OM, Nationale Politie, departementen Financiën en Sociale Zaken en Werkgelegenheid. De deelnemers kunnen per LSI-project verschillen.	Voorkomen en terugdringen van belasting- en premiefraude, uitkeringsfraude, illegale tewerkstelling en daarmee samenhangende misstanden. Dit kan gebeuren vanuit een branche, doelgroep, fenomeen of stedelijk gerichte optiek.
Veiligheidshuizen	Gemeenten, Nationale Politie, OM, Raad voor de Kinderbescherming, Reclasseringsorganisaties, Welzijnsorganisaties.	Veiligheidshuizen zijn netwerksamenwerkingsverbanden, die partners uit de strafrechtketen, de zorgketen, gemeentelijke partners en bestuur verbinden in de aanpak van complexe problematiek. Het doel van de samenwerking is het terugdringen van overlast, huiselijk geweld en criminaliteit.
Regionale hennep convenanten	Gemeenten, Nationale Politie, OM, woningcorporaties, verhuurders, netwerkbedrijven, netbeheerders, UWV, SVB (partijen kunnen variëren per regio/gebied).	Integrale aanpak van hennepkweek om onveilige situaties, criminaliteit en onnodige maatschappelijke kosten terug te dringen.
Stoplicht convenanten	Brancheverenigingen makelaars, politie-eenheden, gemeenten.	Verhinderen dat personen die zich bezighouden met georganiseerde criminaliteit, onroerend goed gebruiken voor criminele activiteiten.
TaskForce Brabant Zeeland	Gemeenten, provincies, OM, Nationale Politie, Belastingdienst, Kmar.	Geïntegreerde aanpak van georganiseerde en ondermijnende criminaliteit in Brabant en Zeeland.
Maritiem Informatieknooppunt (MIK)	NVWA-IOD, Douane, FIOD, RWS, ILT.	In het kader van de nationale veiligheid, het voorkomen van wanordelijkheden, het toezicht op de naleving van wettelijke voorschriften en de opsporing van strafbare feiten de noodzakelijke informatie uitwisselen ten behoeve van de kustwachten laten plaatsvinden.
Infobox Crimineel en Onverklaarbaar Vermogen (iCOV)	Belastingdienst/Belastingen, Belastingdienst/Toeslagen, Belastingdienst/Douane, Belastingdienst/FIOD, FIU-Nederland, Nationale Politie, OM.	In kaart brengen van onverklaarbaar of crimineel vermogen, het blootleggen van witwas- of fraudeconstructies en het kunnen innen van overheidsvorderingen ter

		ondersteuning van de publiekrechtelijke taakuitoefening van de deelnemende organisaties.
Expertisecentrum Zorgfraudebestrijding en fraudeverzamelpunt NZA	NZA, IGZ, Belastingdienst, Inspectie SZW, FIOD, OM, ZN, CIZ, VWS.	Versterking van de integriteit van de zorgsector door samenwerking tussen de convenantpartners te stimuleren, te coördineren en te vergroten door het uitwisselen van informatie en het uitwisselen van kennis, inzicht en vaardigheden.
Nationaal Platform Matchfixing	FP, Belastingdienst, FIOD, Kansspelautoriteit, Politie, KNVB, NOC*NSF, KNLTB en de Lotto.	Verbetering van de informatiepositie van alle stakeholders, zodat meer signalen worden gedetecteerd, meer signalen tijdig via de juiste kanalen bij de juiste stakeholders terecht komen en de meest passende interventie kan worden ingezet.
Hit and Run Cargoteam (HARC)	Douane, FIOD, Zeehavenpolitie.	Onderzoek naar de invoer, uitvoer en doorvoer van verdovende middelen in het havengebied
Contraterrorisme infobox (CT-infobox)	AIVD, MIVD, Nationale Politie, IND, FIU-Nederland, OM.	Leveren van een bijdrage aan de bestrijding van terrorisme door het op een centraal punt bij elkaar brengen en vergelijken van informatie over netwerken en personen die op één of andere wijze betrokken zijn bij terrorisme, in het bijzonder islamitisch terrorisme, en de daaraan te relateren radicalisering.
Electronic Crimes Taskforce (ECTF)	Nationale Politie, Landelijk Parket, banken en Centre for Protection of the National Infrastructure (CPNI).	Veilig en betrouwbaar betalingsverkeer is van groot belang voor de stabiliteit en integriteit van het financiële stelsel. De samenwerking in de ECTF brengt daarvoor unieke en specifieke kennis, informatie en expertise samen. Dat zorgt voor betere analyses en versterking van de informatiepositie om cybercrime aan te vallen.
Landelijk Informatiecentrum Voertuigcriminaliteit	RDW, Nationale Politie, de Stichting Verzekeringsbureau Voertuigcriminaliteit (VbV) en de Belastingdienst.	Informatie- en kenniscentrum dat een bijdrage levert aan de opsporing en bestrijding van voertuigcriminaliteit door vroegtijdige signalering van dergelijke criminaliteit.
Landelijk Skimmingpoint	Minister V&J, Nationale Politie, OM, NVB, Equens SE, Betaalvereniging Nederland.	Publiek-private bestrijding van fraude door skimming.
Nationaal Platform Criminaliteitsbeheersing/ Regionale Platforms Criminaliteitsbeheersing	Minister van V&J, Minister EZ, VNO/NCW, MKB-Nederland, Nederlandse Vereniging van Banken, Korpschef Nationale Politie, Koninklijke Horeca Nederland, VNG, Verbond van Verzekeraars, OM, Detailhandel Nederland.	• Bestuderen en analyseren van de criminaliteitspatronen die de Nederlandse samenleving en in het bijzonder het Nederlandse bedrijfsleven bedreigen; • Versterken van de beveiligingsfunctie in de breedste zin van bedrijven en instellingen door middel van bijvoorbeeld advisering, deskundigheids-bevordering, voorlichting en de normalisatie en certificering van

		beveiligingsprodukten en -diensten; • Bijdragen aan een effectieve preventie en rechtshandhaving met betrekking tot tegen het bedrijfsleven gerichte criminaliteit door middel van advisering van de Ministers van V&J en EZ, het OM, het binnenlands bestuur en de politie; • Bevorderen van de onderlinge samenhang tussen de beveiligingsinspanningen van het bedrijfsleven en de rechtshandhavingsinspanningen van de overheid ter vergroting van hun doelmatigheid en effectiviteit door middel van advisering over bijvoorbeeld prioriteitenstelling en het opzetten van proefprojecten.
Convenant aanpak ram- en plofkraken	Banken, de Nationale Politie en OM.	Door het sneller uitwisselen van informatie ontstaat er sneller en beter inzicht in trends en gebruikte modus operandi van potentiele daders. Hierdoor worden voorzorgsmaatregelen getroffen en wordt de opsporing makkelijker.
Convenant aanpak Verzekeringsfraude	Verbond van Verzekeraars, Zorgverzekeraars Nederland, OM en Nationale Politie.	Terugdringen van verzekeringsfraude door: 1. beter zicht te krijgen op verzekeringsfraude; 2. te komen tot een integrale, programmatische aanpak, bestaande uit preventie, detectie, civielrechtelijke en strafrechtelijke afhandeling en 3. het proces van meldingen, aangiftes en strafrechtelijke afdoening te stroomlijnen.
Landelijk Meldpunt Internetoplichting	Nationale Politie, Rabobank, ABN-AMRO, ING, SNS (alle vertegenwoordigd door NVB), en OM.	Zicht op aard en omvang van oplichting in het online private handelsverkeer, teneinde te komen tot integrale programmatische aanpak van oplichting in het online handelsverkeer door middel van preventie, detectie en strafrechtelijke handhaving, stroomlijnen van proces van meldingen, aangiftes en strafrechtelijke handhaving.
Suwinet-inkijk	Verschillende bronnen (GBA, DUO, Kadaster, RDW) en gebruikers (gemeenten, SVB, UWV).	Suwinet-Inkijk biedt overheidsorganisaties de mogelijkheid om voor hun wettelijke taakuitoefening gegevens van burgers die bij andere overheidsorganisaties of basisregistraties zijn opgeslagen, te raadplegen in een webtoepassing.
Inspectieview Milieu	Partijen bestaan uit bronhouders en gebruikers. Sinds november 2013 hebben de volgende partijen een	Verbeteren aanpak milieuovertredingen. Gegevens worden door middel van Inspectieview Milieu uitsluitend

	aansluitovereenkomst getekend: ILT, NVWA, Inspectie SZW, DCMR (omgevingsdienst) en OZHZ (omgevingsdienst).	verwerkt ten behoeve van vergunningverlening aan, verwerken van meldingen van en toezicht op bedrijven en andere organisaties die activiteiten verrichten waarop de milieuwetgeving van toepassing is alsmede het handhaven in verband daarmee van wettelijke voorschriften.
Convenant samenwerking en informatie-uitwisseling bestrijding gewelddadige vermogenscriminaliteit gericht op de financiële sector	Rabobank, SNS, ING, ABN-AMRO, Nationale Politie en OM.	Uitbouwen samenwerking tussen publieke en private partijen met het oog op de bestrijding van gewelddadige vermogenscriminaliteit gericht op de financiële sector. Het convenant behelst de vastlegging van de wens om binnen de wettelijke kaders en gelet op het publieke en/of maatschappelijke taak en verantwoordelijkheid die elk der convenantpartners in het kader van de voorkoming en bestrijding van deze vorm van criminaliteit heeft, unieke en organisatiespecifieke kennis, informatie en expertise met elkaar te delen.